on networks™
Easy, Reliable & Secure

N300 WiFi ADSL2+ Modem Router (N300RM)

User Manual

December 2012
202-11208-01
v1.0

Trademarks

Brand and product names are trademarks or registered trademarks of their respective holders. Information is subject to change without notice.

In the interest of improving internal design, operational function, and/or reliability, On Networks reserves the right to make changes to the products described in this document without notice. On Networks does not assume any liability that may occur due to the use or application of the product(s) or circuit layout(s) described herein.

Contents

Chapter 1 Hardware Setup

Unpack Your Modem Router 8
Position Your Modem Router 8
Hardware Features 9
Front Panel 9
Back Panel 10
Reset Button on the Side Panel 11
Label 11
ADSL Microfilters 12
One-Line ADSL Microfilter 12
Two-Line ADSL Microfilter 13
Cable Your Modem Router 13
Tips for Connecting to the Modem Router 16

Chapter 2 Getting Started

Modem Router Setup Preparation 18
Use Standard TCP/IP Properties for DHCP 18
Gather ISP Information 18
Wireless Devices and Security Settings 18
Types of Logins and Access 18
Log In to the Modem Router 19
Unsuccessful Login 20
Log Out Manually 20
Upgrade the Firmware 20
Home Screen (Dashboard) 21
EZ Setup Wizard 22
Join Your Wireless Network 23
WPS Method 23
Manual Method 24

Chapter 3 Modem Router Setup

Internet Setup (Basic Settings) 26
ADSL Settings 28
Preset Security 29
Wireless Security Basics 29
Disable SSID Broadcast 29
Restrict Access by MAC Address 30
Wireless Security Options 30
Wireless Setup 30

Consider Every Device on Your Network 31
View or Change Wireless Settings 31
Wireless Settings Screen Fields 32
Change WPA Security Option and Passphrase 32
Guest Network 33
WAN Setup 33
Default DMZ Server 34
Change the MTU Size 35
LAN Setup 36
Use the Modem Router as a DHCP Server 38
Address Reservation 39
Quality of Service (QoS) Setup 39

Chapter 4 Security Settings

Firewall Rules to Control Network Access 44
Inbound Rules (Port Forwarding) 44
Outbound Rules (Service Blocking) 44
Block Internet Sites 45
Firewall Rules to Control Network Access 46
Set Up Firewall Rules 46
Set the Time Zone 47
Schedule Blocking and Services 48
Set Up Email Alerts 49
Port Forwarding and Port Triggering 50
Remote Computer Access Basics 50
Port Triggering to Open Incoming Ports 52
Port Forwarding to Permit External Host Communications 53
How Port Forwarding Differs from Port Triggering 54
Set Up Port Forwarding to Local Servers 54
Add a Custom Service 55
Edit or Delete a Port Forwarding Entry 56
Application Example: Making a Local Web Server Public 56
Set Up Port Triggering 56

Chapter 5 Network Management

Upgrade the Modem Router Firmware 60
Automatic Firmware Check 60
Check for Firmware Upgrades 61
Backup Settings 61
Back Up 62
Restore 62
Erase 62
Change Password 62
Password Recovery 63
View Router Status 64
Router Information 64
Internet Port Settings 64

Wireless Settings and Guest Network (2.4GHz) 66
View Attached Devices 67
Logs 67

Chapter 6 Advanced Settings

Advanced Wireless Settings 70
Restrict Wireless Access by MAC Address 71
Wireless Repeating (WDS) 72
Wireless Repeating 73
Set Up the Base Station 74
Set Up a Repeater Unit 75
Dynamic DNS 75
Static Routes 76
Remote Management 78
Universal Plug and Play 79
Change the Device Mode 80

Chapter 7 Virtual Private Networking

Set Up a Gateway-to-Gateway VPN Configuration 82
VPN Wizard 83
Activate the VPN Tunnel 85
Verify the Status of a VPN Tunnel 86
Deactivate a VPN Tunnel 86
Use Auto Policy to Configure VPN Tunnels 88
Use Manual Policy to Configure VPN Tunnels 91

Chapter 8 Troubleshooting

Troubleshoot with the LEDs 95
Power LED Is Off 95
Power LED Is Red 95
Ethernet LED Is Off 96
Cannot Log In to the Modem Router 96
Troubleshoot the Internet Connection 97
ADSL Link 97
Internet LED Is Red 98
Obtain an Internet IP Address 98
Troubleshoot PPPoE or PPPoA 98
Troubleshoot Internet Browsing 99
TCP/IP Network Not Responding 99
Test the LAN Path to Your Modem Router 99
Test the Path from Your Computer to a Remote Device 100
Changes Not Saved 101
Incorrect Date or Time 101

Appendix A Supplemental Information

Factory Settings 103
Technical Specifications 105

Appendix B Notification of Compliance

Hardware Setup

1

Getting to know your modem router

The N300 WiFi ADSL2+ Modem Router (N300RM) provides you with an easy and secure way to set up a wireless home network with fast access to the Internet over a high-speed digital subscriber line (DSL). The modem router has a built-in DSL modem and is compatible with all major DSL Internet service providers. With your modem router, you can block unsafe Internet content and applications, and protects the devices (computers, gaming consoles, and so on) that you connect to your home network.

This chapter explains how to set up your hardware. If you have already set up your modem router, you can skip this chapter. Chapter 2 explains how to set up your Internet connection.

This chapter contains the following sections:

- *Unpack Your Modem Router*
- *Position Your Modem Router*
- *Hardware Features*
- *ADSL Microfilters*
- *Cable Your Modem Router*

Unpack Your Modem Router

Open the box and remove the modem router, cables, and installation guide.

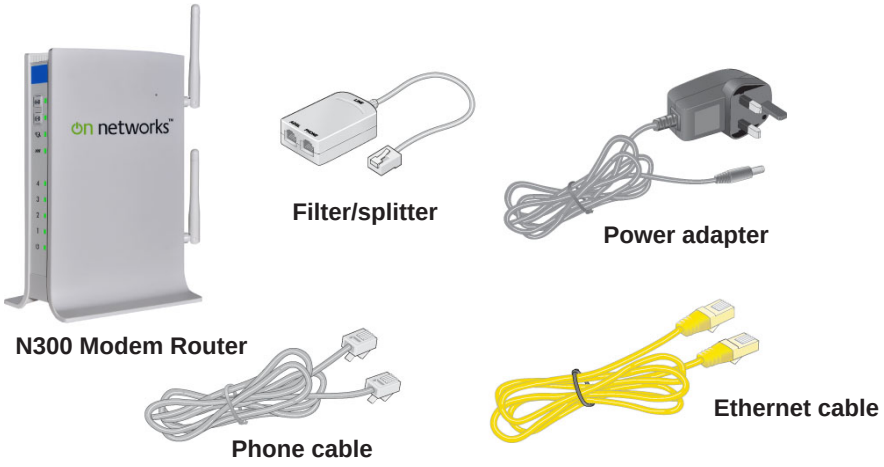


Figure 1. Check the package contents

If any parts are incorrect, missing, or damaged, contact your On Networks dealer. Keep the carton and original packing materials in case you need to return the product for repair.

Position Your Modem Router

The modem router lets you access your network anywhere within the operating range of your wireless network. However, this distance can vary significantly depending on where you put your modem router. For example, the thickness and number of walls the wireless signal passes through can limit the range. For best results, place your modem router:

- Near the center of the area where your computers and other devices operate and preferably within line of sight to your wireless devices.
- So it is accessible to an AC power outlet and near Ethernet cables for wired computers.
- In an elevated location such as a high shelf, keeping the number of walls and ceilings between the modem router and your other devices to a minimum.
- Away from electrical devices that are potential sources of interference. Equipment that might cause interference includes ceiling fans, home security systems, microwaves, computers, the base of a cordless phone or 2.4 GHz cordless phone.
- Away from any large metal surfaces, such as a solid metal door or aluminum studs. Large expanses of other materials such as glass, insulated walls, fish tanks, mirrors, brick, and concrete can also affect your wireless signal.

When you use multiple access points, it is better if adjacent access points use different radio frequency channels to reduce interference. The recommended channel spacing between adjacent access points is 5 channels (for example, use Channels 1 and 6, or 6 and 11).

Hardware Features

Before you cable your modem router, take a moment to become familiar with the front, side, and back panels and the label. Pay particular attention to the LEDs on the front panel.

Front Panel

The modem router front panel has two buttons and status LEDs.

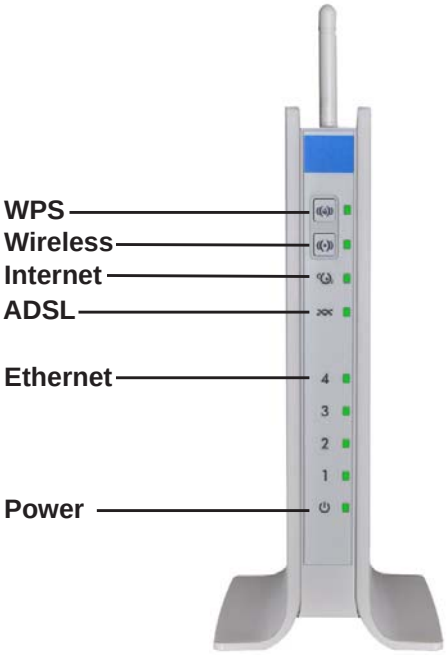


Figure 2. Modem router front panel

Table 1. Button and LED descriptions

Icon	Description
WPS 	Wi-Fi Protected Setup (WPS) lets you join a secure wireless network without typing the password. See *WPS Method* on page 23. • **Solid green**. A WPS-capable device is connected to the router. • **Blinking green**. WPS connection with WPS-capable device is in process. • **Off**. No WPS connection.
Wireless 	You can press the Wireless button to turn the wireless radio off and on. • **Blinking green**. Data is being transmitted or received over the wireless link. • **Off**. The wireless radio is turned off.
Internet 	• **Solid green**. The Internet connection has been established. • **Blinking green**. There is traffic on the Internet port. • **Solid red**. The Internet connection failed. • **Off**. No Internet connection.

Table 1. Button and LED descriptions (continued)

Icon	Description
ADSL 	• **Solid green**. You have a DSL connection. In technical terms, the DSL port is synchronized with an ISP's network-access device. • **Blinking green**. The modem router is negotiating the best possible speed on the DSL line. • **Off**. The unit is off or there is no DSL link established.
Ethernet (1-4) 	• **Solid green**. The LAN port has detected an Ethernet link with a device such as a computer. • **Blinking green**. Data is being transmitted or received. • **Off**. No link is detected on this port.
Power/ Check 	• **Solid green**. Power is supplied to the modem router. • **Blinking green**. The router is starting up. • **Solid red**. Power-on self-test (POST) failed or a device malfunction has occurred. • **Off**. Power is not supplied to the modem router.

Back Panel

The back panel has the connections shown in the following figure.

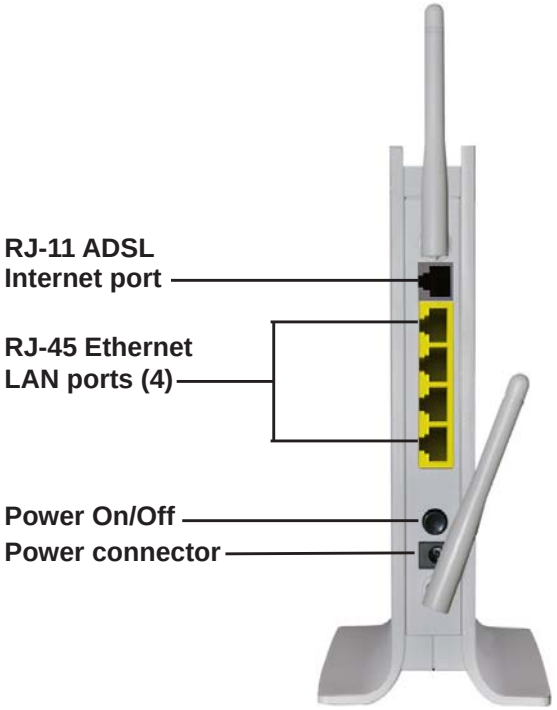
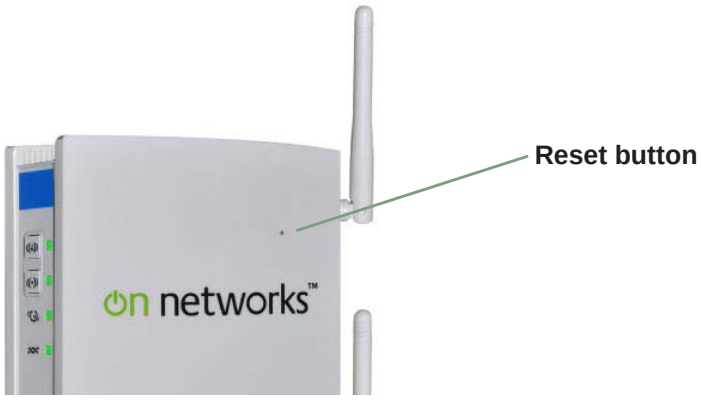


Figure 3. Router, back panel

See *Factory Settings* on page 103 for information about restoring factory settings.

Reset Button on the Side Panel

You can use the Reset button to return the modem router to its factory settings.



- **To reset the modem router:**

  Use a pin or paper clip to press and hold the **Reset** button for at least 7 seconds.

For information about the factory settings, see *Factory Settings* on page 103.

Label

The label on the bottom of the modem router shows the preset WiFi network name and password, login information, MAC address, and serial number.

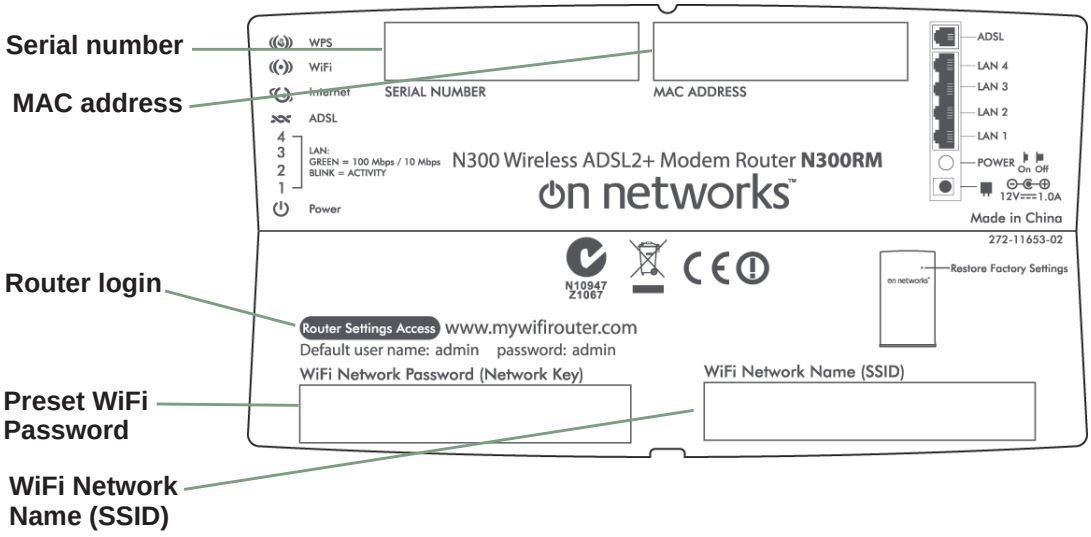


Figure 4. The label shows unique information about your modem

ADSL Microfilters

The first time you cable a wireless modem between a DSL phone line and your computer or laptop, you might not be familiar with ADSL microfilters. If you are, you can skip this section and proceed to *Cable Your Modem Router* on page 13.

An ADSL microfilter is a small inline device that filters DSL interference out of standard phone equipment that shares the same line with your DSL service. Every telephone device that connects to a telephone line that provides DSL service needs an ADSL microfilter to filter out the DSL interference. Example devices are telephones, fax machines, answering machines, and caller ID displays. Not every phone line in your home necessarily carries DSL service. The need for DSL service depends on the DSL service setup in your home.

Note: Often the ADSL microfilter is in the box with the modem router. If you purchased the modem router in a country where a microfilter is not included, purchase the ADSL microfilter separately.

One-Line ADSL Microfilter

➢ **To use a one-line ADSL microfilter:**

1. Plug the ADSL microfilter into the DSL line outlet on the wall.
2. Plug your phone equipment into the jack labeled Phone.

   The modem router plugs directly into a separate DSL line. If you plug the wireless modem router into the phone jack, it blocks the Internet connection.

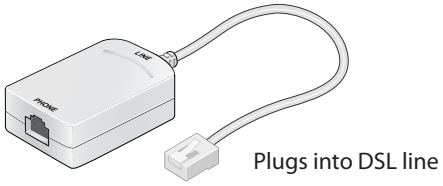


Figure 5. One-line ADSL microfilter

If you do not have a separate DSL line for the modem, the best thing to do is to use an ADSL microfilter with a built-in splitter. See *Two-Line ADSL Microfilter* on page 13. You can also purchase a separate splitter.

➢ **To use a separate splitter:**

1. Insert the splitter into the phone outlet.
2. Connect the one-line filter to the splitter.
3. Connect the phone to the filter.
4. Plug the modem into one of the other outlets in the separate splitter.

Two-Line ADSL Microfilter

Use an ADSL microfilter with a built-in splitter when there is a single wall outlet that provides connectivity for both the modem router and your telephone equipment.

➢ **To use a two-line ADSL microfilter:**

1. Plug the ADSL microfilter into the DSL outlet on the wall.
2. Plug your phone equipment into the jack labeled Phone.
3. Plug the wireless modem modem into the jack labeled ADSL.

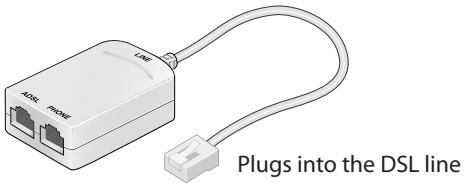


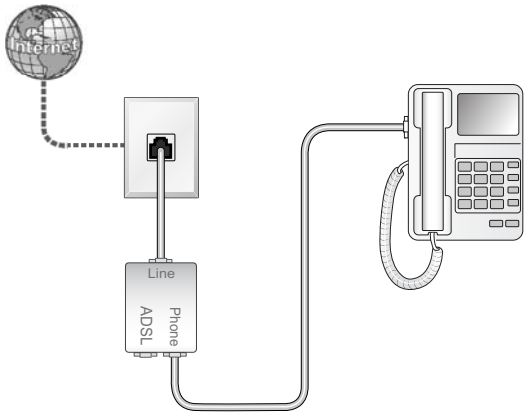
Figure 6. Two-line ADSL microfilter with built-in splitter

Cable Your Modem Router

The installation guide that came in the box has a cabling diagram. This section walks you through how to cable your modem with detailed illustrations.

➢ **To cable your modem:**

1. Put an ADSL microfilter between the phone line and the phone as shown here. The illustration shows a two-line ADSL microfilter with a built-in splitter. The phone plugs into the Phone jack as shown.

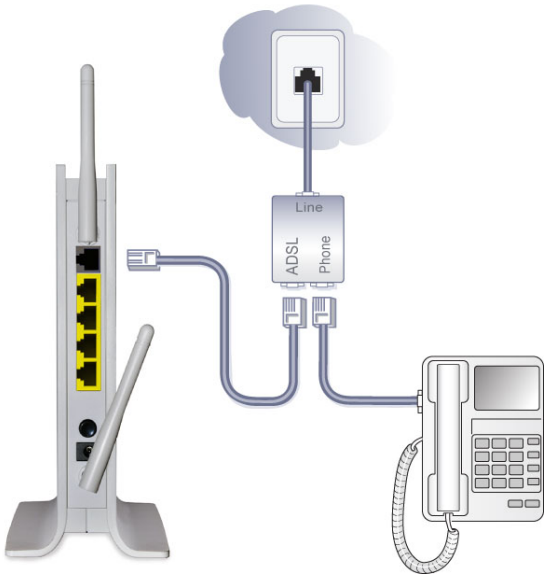


2. Use the included phone cable with RJ-11 jacks to connect the ADSL port (A) of the modem router to the ADSL port (B) of the two-line ADSL microfilter.

CAUTION:

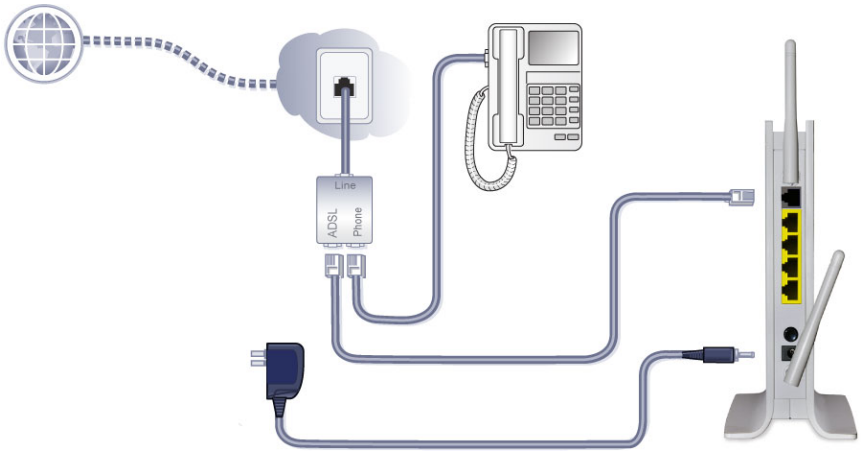
Incorrectly connecting a filter to your modem router blocks your DSL connection.

3. Connect the ADSL port of the modem router to the ADSL port of the filter/splitter.



If your modem router and telephone connect to the same phone line, use an ADSL filter/splitter for every phone line in the house.

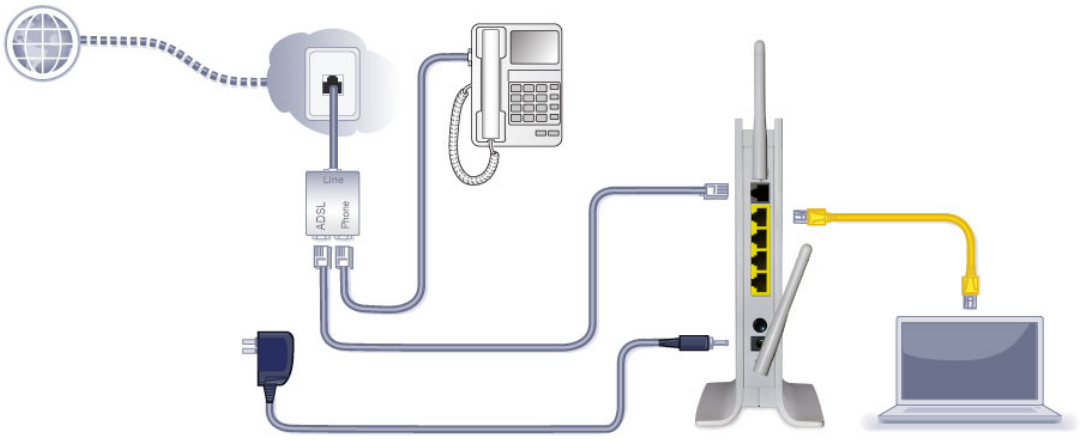
4. Add power to the modem router.



a. Connect the power adapter to the router, and plug the power adapter into an outlet.
b. Wait for the Wireless LED on the front panel to light. If no LEDs are lit, press the **Power On/Off** button on the rear panel of the modem router.

5. Connect a computer.

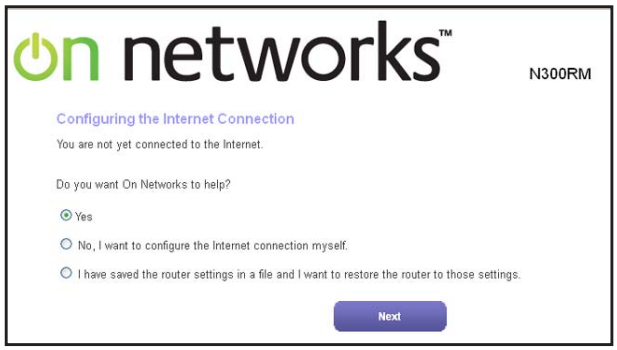
   You can use an Ethernet cable or connect wirelessly.



   - Use the yellow Ethernet cable to connect your computer to an Ethernet port on your modem.
   - Or connect wirelessly by using the preset wireless security settings on the label on the bottom of the router.

6. Open a browser.

   The first time that you connect to your modem, the browser automatically displays a modem routerscreen to help you set up your Internet connection.



   If this screen does not display, see the following section, *Tips for Connecting to the Modem Router* on page 16.

   If you already connected to the modem and used this screen, you are prompted to log in. See *Log In to the Modem Router* on page 19.

7. Connect any additional wired computers to your modem router by inserting an Ethernet cable from a computer into one of the three remaining LAN ports.

   Note: *To use the modem router on the same network as another router, you need to change the Device Mode setting to Modem mode. See Change the Device Mode on page 102.*

Tips for Connecting to the Modem Router

If the browser cannot display the web page:

- Make sure that the computer is connected to one of the four LAN Ethernet ports or wirelessly to the modem router.
- Make sure that the modem has full power, and that its Wireless LED is lit.
- Close and reopen the browser to make sure that the browser does not cache the previous page.
- Browse to **http://www.mywifirouter.com** (or **http://192.168.0.1/index.htm**).
- If the computer is set to a static or fixed IP address (this is uncommon), change it to obtain an IP address automatically from the modem router.

If the modem router does not connect to the Internet:

1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.

Getting Started

2

Accessing your modem

This chapter explains how to access and set up your modem router after you complete cabling as described in the installation guide and in the previous chapter.

This chapter contains the following sections:

- *Modem Router Setup Preparation*
- *Types of Logins and Access*
- *Log In to the Modem Router*
- *Upgrade the Firmware*
- *Home Screen (Dashboard)*
- *EZ Setup Wizard*
- *Join Your Wireless Network*

Modem Router Setup Preparation

Before you start the setup process, get your ISP information and make sure the computers and devices in the network have the settings described here.

Use Standard TCP/IP Properties for DHCP

If you set up your computer to use a static IP address, change the settings so that it uses Dynamic Host Configuration Protocol (DHCP).

Gather ISP Information

If you have DSL broadband service, you might need the following information to set up your modem router and to check that your Internet configuration is correct. Your Internet service provider (ISP) should have provided you with all of the information to connect to the Internet. If you cannot locate this information, ask your ISP to provide it. When your Internet connection is working, you no longer launch the ISP login program on your computer to access the Internet. When you start an Internet application, your modem router automatically logs you in. Make sure that you have the following information:

- The ISP configuration information for your DSL account
- ISP login name and password
- Fixed or static IP address settings (special deployment by ISP [rare])

Wireless Devices and Security Settings

Make sure that the wireless device or computer that you are using supports WPA or WPA2 wireless security, which is the wireless security that the modem router supports.

Types of Logins and Access

There are separate types of logins that have different purposes. It is important that you understand the difference so that you know which login to use when.

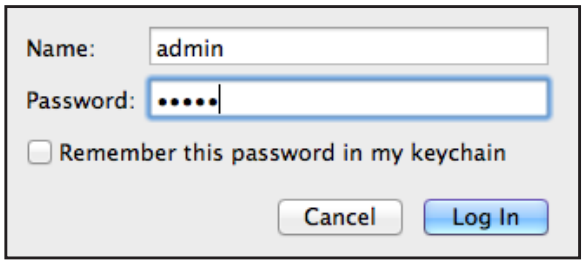
- **Modem router login** logs you in to the modem router interface.
- **ISP login** logs you in to your Internet service. Your service provider has provided you with this login information in a letter or some other way. If you cannot find this login information, contact your service provider.
- **Wireless network key or password**. Your modem router is preset with a unique wireless network name (SSID) and password for wireless access. This information is on the label on the bottom of your modem router.

Log In to the Modem Router

The first time that you connect to the modem router, the installation screen displays. After initial setup, you can log in to the modem router to view or change its settings.

➢ **To log in:**

1. With an Internet browser, browse to **http://www.mywifirouter.com** (or **http://192.168.0.1/index.htm**).



2. Enter **admin** for the user name and **admin** for the password, both in lowercase letters.

Note: As explained in the previous section, the modem router user name and password are different from the user name and password for logging in to your Internet connection.

When you log in, if you are connected to the Internet, the Firmware Upgrade Assistant screen displays so you can upgrade to the latest firmware.

A message displays telling you whether the router discovered a newer version of firmware.

3. To update to the new firmware, click **Yes** to allow the router to download and install the new firmware file from On Networks.

WARNING:

When uploading firmware to the modem router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

When the upload is complete, your modem router restarts. The update process typically takes about 1 minute.

Unsuccessful Login

- **Do the following if you do not see the login prompt:**

1. Check the LEDs on the front of the modem router to make sure that the modem router is plugged in, its power is on, and the Ethernet cable between your computer and the modem router is connected to a LAN port.
2. If you connected the Ethernet cable and quickly launched your browser and typed in the modem router URL, your computer might need a minute or two to recognize the LAN connection. Relaunch your browser and try again.
3. If you are having trouble accessing the modem router wirelessly, On Networks recommends that during setup you use an Ethernet cable to connect your computer so that you can log in to the modem router.
4. If you cannot connect to the modem router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your Windows computer Control Panel. They should be set to obtain both IP and DNS server addresses automatically. See your computer documentation.

Log Out Manually

The modem router interface provides a Logout command at the bottom of the modem router menus. Log out when you expect to be away from your computer for a relatively long time.

Upgrade the Firmware

When you log in, if you are connected to the Internet, the Firmware Upgrade Assistant screen displays so you can upgrade to the latest firmware.

- **To upgrade the firmware:**

1. Click **Yes** to check for new firmware (recommended). The modem router checks for new firmware.
2. If no new firmware is available, click **No** to exit. You can check for new firmware later.
3. If new firmware is available, click **Yes** to upgrade the modem router with the latest firmware. After the upgrade, the modem router restarts.

CAUTION:

Do not try to go online, turn off the modem router, shut down the computer, or do anything else to the modem router until the modem router finishes restarting and the Power LED has stopped blinking for several seconds.

You cannot upgrade firmware until you have established your Internet connection as described in *EZ Setup Wizard* on page 22.

Home Screen (Dashboard)

The modem router interface lets you view or change the modem router settings. The left column has menus. The main screen is the currently selected menu option.

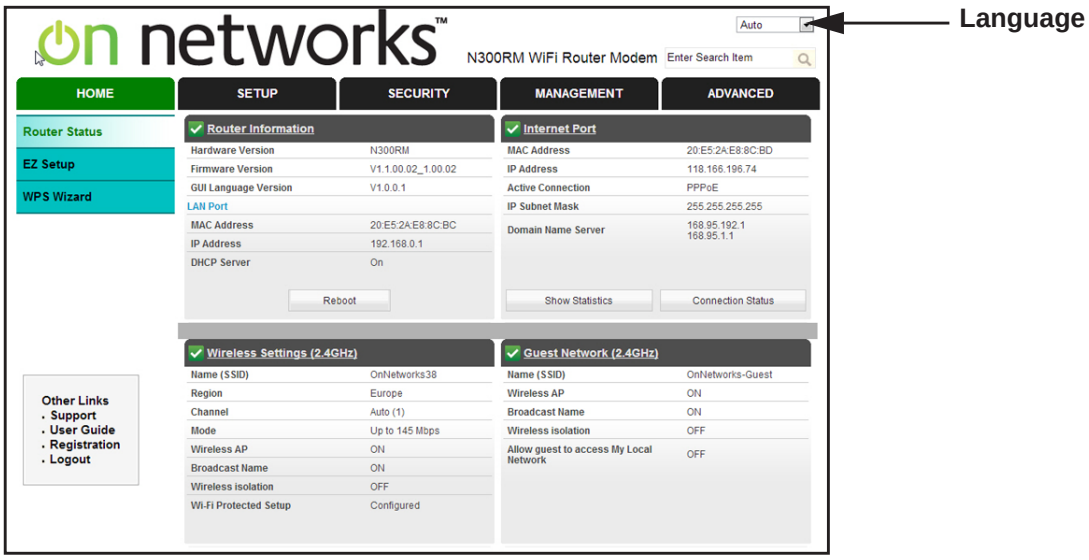


Figure 7. Dashboard (Home screen)

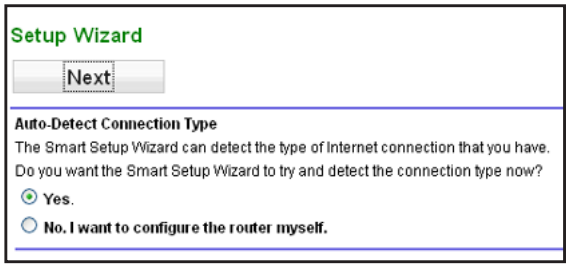
- **EZ Setup Wizard**. Specify the language and location, and automatically detect the Internet connection. See *EZ Setup Wizard* on page 22.
- **WPS Setup**. Join the secure WiFi network without typing the password. See *Join Your Wireless Network* on page 23.
- **Setup tab**. Set, upgrade, and check the ISP and wireless network settings of your modem router. See *Chapter 3, Modem Router Setup*.
- **Security tab**. View and configure the modem router firewall settings to prevent objectionable content from reaching your computers. See *Chapter 4, Security Settings*.
- **Management tab**. Administer your modem router and network. See *Chapter 5, Network Management*.
- **Advanced tab**. Set the modem router up for unique situations such as when remote access by IP or by domain name from the Internet is needed. Using this menu requires a solid understanding of networking concepts. See *Chapter 6, Advanced Settings*.
- **Other Links**. Go to the support site to get information, help, and product documentation. These links work once you have an Internet connection.

EZ Setup Wizard

You can log in to the modem router and use EZ Setup to set up your Internet connection.

➢ **To use the EZ Setup wizard:**

1. From the top of the modem router menu, select **EZ Setup** to display the following screen:



2. Select either **Yes** or **No, I want to configure the router myself**. If you select No, proceed to *Internet Setup (Basic Settings)* on page 26.
3. If you selected Yes, click **Next**.

   With automatic Internet detection, the EZ Setup Wizard searches your Internet connection for servers and protocols to determine your ISP configuration.

The EZ Setup Wizard cannot detect a Point-to-Point Tunneling Protocol (PPTP) connection. If your ISP uses PPTP, you have to set your Internet connection through the screen described in *Internet Setup (Basic Settings)* on page 26.

➢ **To troubleshoot an unsuccessful Internet connection:**

1. Review your settings to be sure that you have selected the correct options and typed everything correctly.
2. Contact your ISP to verify that you have the correct configuration information.
3. Read *Chapter 8, Troubleshooting*. If problems persist, register your product and contact technical support.
4. If you cannot connect to the modem router, check the Internet Protocol (TCP/IP) properties in the Network Connections section of your Windows computer Control Panel. They should be set to obtain *both* IP and DNS server addresses automatically. See your computer documentation.

Join Your Wireless Network

Choose either the WPS method or the manual method to join your wireless network.

WPS Method

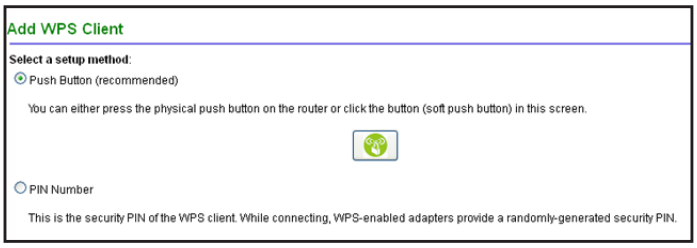
Wi-Fi Protected Setup (WPS) lets you connect to a secure WiFi network without typing its password. Instead, you press a button or enter a PIN. Some older WiFi equipment is not compatible with WPS. WPS works only with WPA2 or WPA wireless security.

➢ **To use the WPS button on the modem router:**

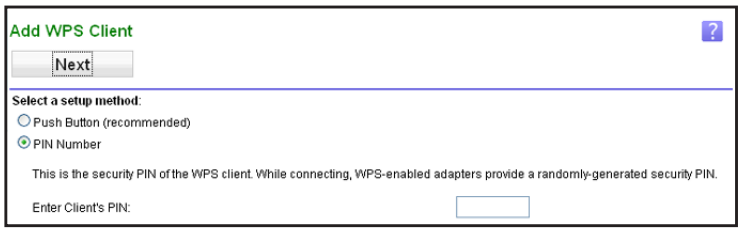
1. Press the  **WPS** button on the front of the modem router.
2. Within 2 minutes, use WPS to join the network using one of the following methods:
   - If your computer or wireless device has a WPS button, press it.
   - On your computer or wireless device, with the software you use to join wireless networks, select the **WPS** option, and follow the instructions to connect.

➢ **To use the WPS method when you are logged in to the modem router:**

1. Select **Home > WPS Setup**.
2. Click **Next**. The following screen lets you select the method for adding the WPS client.



3. Select either **Push Button** or **PIN Number**. With either method, the modem router tries to communicate with the computer or wireless device, set the wireless security for wireless device, and allow it to join the wireless network.
4. When the PIN method screen displays, enter the client security PIN.



When the modem router establishes a WPS connection, the modem router WPS screen displays a confirmation message.

Manual Method

With the manual method, select the network that you want, and type its password to connect.

➢ **To connect manually:**

1. On your computer or wireless device, open the software that manages your wireless connections. This software scans for all wireless networks in your area.
2. Look for your network and select it.

   The unique WiFi network name (SSID) and password are on the router label. If you changed these settings, then look for the network name that you used.
3. Enter the modem router password and click **Connect**.

Modem Router Setup

3

Options on the Setup tab

This chapter contains the following sections:

- *Internet Setup (Basic Settings)*
- *ADSL Settings*
- *Preset Security*
- *Wireless Security Basics*
- *Wireless Setup*
- *Guest Network*
- *WAN Setup*
- *LAN Setup*
- *Quality of Service (QoS) Setup*

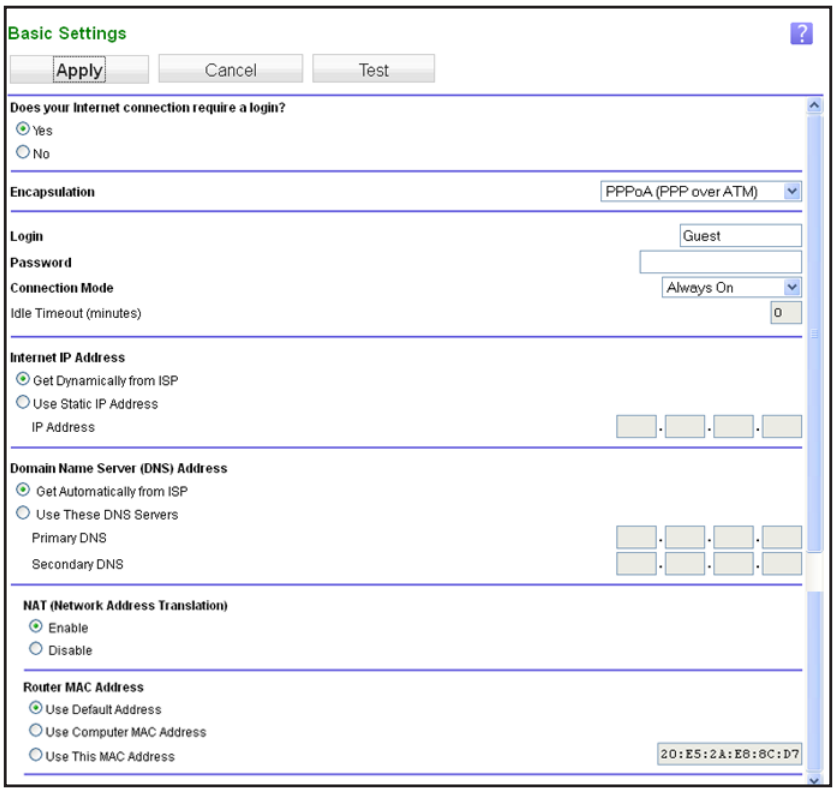
Internet Setup (Basic Settings)

The Basic Settings screen displays when you select No. I want to configure the Router myself in the EZ Setup wizard and is also available from the modem router menu. It is where you view or change ISP information. The fields that display vary depending on whether your Internet connection requires a login.

Note: Check that the country is set before proceeding with the manual setup.

➢ **To manually set up the Internet connection:**

1. Select **Setup > Internet Setup**.



2. Select **Yes** or **No** depending on whether your ISP requires a login.
   - **Yes**. Select the encapsulation method and enter the login name. If you want to change the login time-out, enter a new value in minutes.
   - **No**. Enter the account and domain names, as needed.
3. Enter the settings for the IP address and DNS server. The default DSL settings usually work fine. If you have problems with your connection, check the ISP settings.
4. If no login is required, you can specify the MAC Address setting.

5. Click **Apply** to save your settings.
6. Click **Test** to test your Internet connection. If you are not able to connect within 1 minute, see *Chapter 8, Troubleshooting*.

The following descriptions explain all of the possible fields in the Basic Settings screen. The fields that display in this screen depend on whether an ISP login is required.

Does Your ISP Require a Login? Answer either yes or no.

- *When no login is required, these fields display:*

  Account Name (If required). Enter the account name that your ISP provided. This might also be called the host name.

  Domain Name (If required). Enter the domain name that your ISP provided.

- *When your ISP requires a login, these fields display:*

  Encapsulation. Encapsulation is a method for enclosing multiple protocols. PPP stands for Point-to-Point Protocol. The choices are PPPoE (PPP over Ethernet) or PPPoA (PPP over ATM).

  Login. The login name that your ISP provided. This is often an email address.

  Password. The password that you use to log in to your ISP.

  Service Name (If Required). Enter the account name provided by your ISP. This might also be called the host name.

  Connection Mode. By default, this setting is Always On, so that the modem router automatically connects to the Internet.

  Idle Timeout (In minutes). If you want to change the login timeout, enter a new value in minutes. This determines how long the modem router keeps the Internet connection active after there is no Internet activity from the LAN. Entering a value of 0 (zero) means never log out.

Internet IP Address.

- **Get Dynamically from ISP**. Your ISP uses DHCP to assign your IP address. Your ISP automatically assigns these addresses.
- **Use Static IP Address**. Enter the IP address, IP subnet mask, and the gateway IP address that your ISP assigned. The gateway is the ISP's modem router to which your modem router will connect.

Domain Name Server (DNS) Address. The DNS server is used to look up site addresses based on their names.

- **Get Automatically from ISP**. Your ISP uses DHCP to assign your DNS servers. Your ISP automatically assigns this address.
- **Use These DNS Servers**. If you know that your ISP does not automatically transmit DNS addresses to the modem router during login, select this option, and enter the IP address of your ISP's primary DNS server. If a secondary DNS server address is available, enter it also.

NAT (Network Address Translation). You can enable or disable NAT. If you disable NAT, you can also disable the firewall. The firewall cannot be disabled when NAT is enabled.

Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from working. Open NAT provides a much less secured firewall, but allows almost all Internet applications to work.

Router MAC Address. The Ethernet MAC address used by the modem router on the Internet port. Some ISPs register the MAC address of the network interface card in your computer when your account is first opened. They accept traffic only from the MAC address of that computer. This feature allows your modem router to use your computer's MAC address (this is also called cloning).

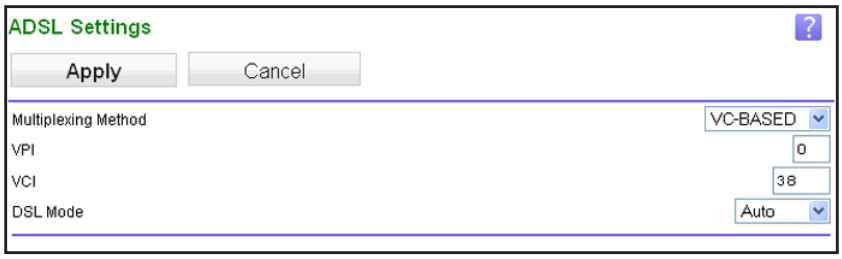
- **Use Default Address**. Use the default MAC address.
- **Use Computer MAC Address**. The modem router captures and uses the MAC address of the computer that you are now using. You must be using the one computer that is allowed by the ISP.
- **Use This MAC Address**. Enter the MAC address that you want to use.

ADSL Settings

The DSL settings of your wireless modem router work fine for most ISPs. However, some ISPs use a specific multiplexing method and virtual circuit number for the virtual path identifier (VPI) and virtual channel identifier (VCI).

➢ **If your ISP gave you a multiplexing method or VPI and VCI number, enter the setting:**

1. Select **Setup > ADSl Settings**:



2. In the Multiplexing Method drop-down list, select **LLC-based** or **VC-based**.
3. For the virtual path identifier (VPI) parameter, type a number from 0 through 255. The default is 8 for the U.S. version, 0 for the worldwide version, and 1 for the German version.
4. For the virtual channel identifier (VCI) parameter, type a number from 32 through 65535. The default is 35 for the U.S. version, 38 for the worldwide version, and 32 for the German version.
5. For DSL Mode, On Networks recommends the default, which is Auto. In Auto mode, the modem chooses the best modulation for you.

- Click **Apply**.

Preset Security

The modem router comes with preset security. This means that the Wi-Fi network name (SSID), passphrase, and security option (encryption protocol) are preset in the factory. You can find the preset SSID and passphrase on the bottom of the unit.

- **WiFi Network Name (SSID)** identifies your network so devices can find it.
- **WiFi Network Password (Network Key)** controls access to your network. Devices that know the SSID and the passphrase can find your wireless network and connect.

Note: The preset SSID and passphrase are uniquely generated for every device to protect and maximize your wireless security.

- **Security option** is the type of security protocol applied to your wireless network. The security protocol in force encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. The preset security option is WPA-PSK/WPA2-PSK mixed mode, described in *Wireless Security Options* on page 30.

The Wireless Settings screen lets you view and change the preset security settings. If you do decide to change your preset security settings, make a note of the new settings and store it in a safe place where you can easily find it.

Wireless Security Basics

Unlike wired network data, wireless data transmissions extend beyond your walls and can be received by any device with a compatible wireless adapter (radio). For this reason, it is very important to maintain the preset security and understand the other security features available to you. Besides the preset security settings described in the previous section, your modem router has the security features described here and in *Chapter 4, Security Settings*.

- Turn off wireless connectivity
- Disable SSID broadcast
- Restrict access by MAC address
- Wireless security options

Disable SSID Broadcast

By default, the modem router broadcasts its WiFi network name (SSID) so devices can find it. If you change this setting to prevent the broadcast, wireless devices cannot find your modem router unless they are configured with the same SSID.

Note: Turning off SSID broadcast nullifies the wireless network discovery feature of some products such as Windows XP, but the data is still fully exposed to a determined snoop using specialized test equipment like wireless sniffers. If you allow the broadcast, be sure to keep wireless security enabled.

Restrict Access by MAC Address

You can enhance your network security by allowing access to only specific computers based on their Media Access Control (MAC) addresses. You can restrict access to only trusted PCs so that unknown computers cannot wirelessly connect to the modem router. The wireless station MAC address filtering adds additional security protection to the wireless security option that you have in force. The access list determines which wireless hardware devices are allowed to connect to the modem router by MAC address. See *Advanced Wireless Settings* on page 70 for the procedure.

Wireless Security Options

A security option is the type of security protocol applied to your wireless network. The security protocol encrypts data transmissions and ensures that only trusted devices receive authorization to connect to your network. There are several types of encryption: Wi-Fi Protected Access II (WPA2), WPA, and Wired Equivalent Privacy (WEP). WPA2 is the latest and most secure, and is recommended if your equipment supports it. WPA has several options including pre-shared key (PSK) encryption and 802.1x encryption for enterprises. It is possible to disable wireless security, but that is not recommended. You can view or change the wireless security options in the Wireless Settings screen. See *Wireless Setup* on page 30.

Wireless Setup

The Wireless Settings screen lets you view or change the wireless network settings. Your preset modem router has a unique network name and password on the product label. If you decide to change them, note the new settings and save them in a secure location.

If you use a wireless computer to change the wireless network name (SSID) or security options, you are disconnected when you click Apply. To avoid this problem, use a computer with a wired connection to access the modem router.

Consider Every Device on Your Network

Before you begin, check the following:

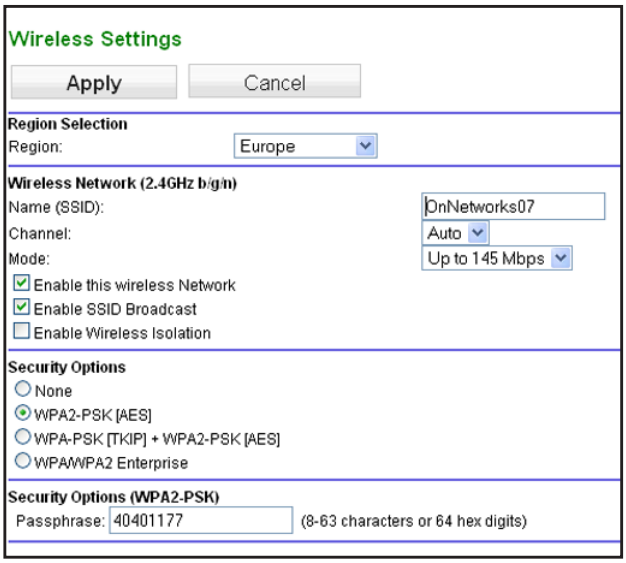
- Every wireless computer has to be able to obtain an IP address by DHCP from the modem router as described in *Use Standard TCP/IP Properties for DHCP* on page 18.
- Each computer or wireless adapter in your network must have the same SSID and wireless mode (bandwidth and data rate) as the modem router. Check that the wireless adapter on each computer can support the mode and security option you want to use.
- The security option on each wireless device in the network must match the modem router. For example, if you select a security option that requires a passphrase, be sure to use the same passphrase for each wireless computer in the network.

View or Change Wireless Settings

Your preset modem router comes set up with a unique wireless network name (SSID) and network password. This information is printed on the label for your modem router. You view or change these settings in the Wireless Settings screen.

➢ **To view or change wireless settings:**

1. Select **Setup > Wireless Settings** to display the following screen.



2. Make any changes that are needed, and click **Apply** when done to save your settings.

> **Note:** The screen sections, settings, and procedures are explained in the following sections.

3. Set up and test your computers for wireless connectivity:

a. Use your wireless computer or device to join your network. When prompted, enter the network password.

b. From the wirelessly connected computer, make sure that you can access the Internet.

Wireless Settings Screen Fields

- **Enable SSID Broadcast**. This setting allows the modem router to broadcast its SSID so that a wireless station can display this wireless name (SSID) in its scanned network list. This check box is selected by default. To turn off the SSID broadcast, clear the check box and click **Apply**.
- **Name (SSID)**. The SSID is also known as the wireless network name. Enter a 32-character (maximum) name in this field. This field is case-sensitive. The default SSID is randomly generated, and there is typically no need to change it.
- **Region**. The location where the modem router is used. It might not be legal to operate the modem router in a region other than the regions listed.
- **Channel**. The wireless channel used by the gateway: 1 through 13. Do not change the channel unless you experience interference (shown by lost connections or slow data transfers). If this happens, experiment with different channels to see which is the best.
- **Mode**. Up to 145 Mbps is the default and allows 802.11n and 802.11g wireless devices to join the network. g & b supports up to 54 Mbps. Up to 300 Mbps supports up to 300 Mbps.

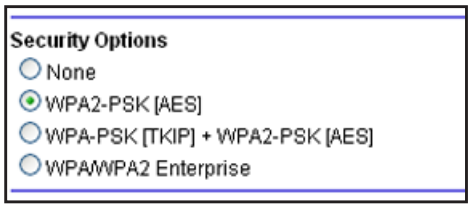
Security Options Settings

The Security Options section of the Wireless Settings screen lets you change the security option and passphrase. Your preset modem router is already set up with WPA2 and WPA security. For information about changing these settings, see the following section, *Change WPA Security Option and Passphrase*.

Change WPA Security Option and Passphrase

➢ **To change WPA security:**

1. In the Security Options section, select the WPA option that you want.



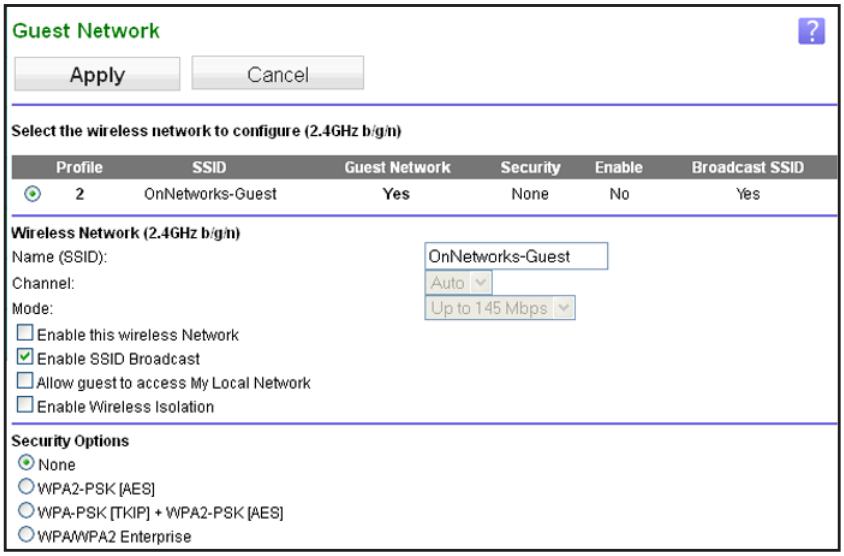
2. Enter the passphrase that you want to use. It is a text string from 8 to 63 characters.
3. Click **Apply**.

Guest Network

You can set up a guest network to allow others to use your Internet connection.

➢ **To set up a guest network:**

1. Select **Basic > Guest**.



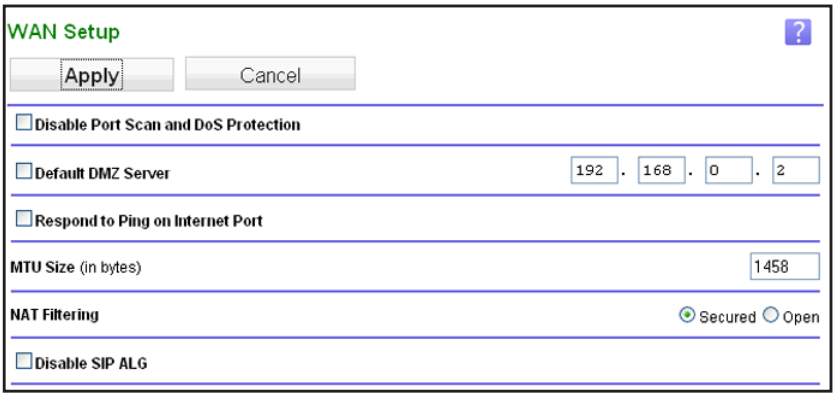
2. Select the check boxes and radio buttons to specify the settings for your guest network.

   The settings are similar to those in the Wireless Settings screen. See *Wireless Setup* on page 30.

3. Click **Apply**.

WAN Setup

The WAN Setup screen lets you configure a DMZ (demilitarized zone) server, change the maximum transmit unit (MTU) size, and enable the modem router to respond to a ping on the WAN (Internet) port. Select **Setup > Internet Port** to view the following screen:



- **Disable Port Scan and DoS Protection**. DoS protection protects your LAN against denial of service attacks such as Syn flood, Smurf Attack, Ping of Death, Teardrop Attack, UDP Flood, ARP Attack, Spoofing ICMP, Null Scan, and many others. This should be disabled only in special circumstances.
- **Default DMZ Server**. This feature is sometimes helpful when you are playing online games or videoconferencing. Be careful when using this feature because it makes the firewall security less effective. See the following section, *Default DMZ Server*, for more details.
- **Respond to Ping on Internet Port**. If you want the modem router to respond to a ping from the Internet, select this check box. Use this setting only as a diagnostic tool because it allows your modem router to be discovered. Do not select this check box unless you have a specific reason.
- **MTU Size (in bytes)**. The normal MTU (maximum transmit unit) value for most Ethernet networks is 1500 bytes or 1492 bytes for PPPoE connections. For some ISPs, you might need to reduce the MTU. This is rarely required. You should reduce the MTU only if you are sure that it is necessary for your ISP connection. See *Change the MTU Size* on page 35.
- **NAT Filtering**. Network Address Translation (NAT) determines how the modem router processes inbound traffic. Secured NAT provides a secured firewall to protect the computers on the LAN from attacks from the Internet, but might prevent some Internet games, point-to-point applications, or multimedia applications from functioning. Open NAT provides a much less secured firewall, but allows almost all Internet applications to function.
- **Disable SIP ALG**. The Session Initiation Protocol (SIP) Application Level Gateway (ALG) is enabled by default to optimize VoIP phone calls that use the SIP. Select the **Disable SIP ALG** check box to disable the SIP ALG. Disabling the SIP ALG might be useful when running certain applications.

Default DMZ Server

The default DMZ server feature is helpful when you are using some online games and videoconferencing applications that are incompatible with Network Address Translation (NAT). The modem router is programmed to recognize some of these applications and to work correctly with them, but there are other applications that might not function well. In some cases, one local computer can run the application correctly if that computer's IP address is entered as the default DMZ server.

WARNING:

DMZ servers pose a security risk. A computer designated as the default DMZ server loses much of the protection of the firewall and is exposed to exploits from the Internet. If compromised, the DMZ server computer can be used to attack other computers on your network.

The router usually detects and discards incoming traffic from the Internet that is not a response to one of your local computers or a service that you have configured in the Port Forwarding/Port Triggering screen. Instead of discarding this traffic, you can have the router forward the traffic to one computer on your network. This computer is called the default DMZ server.

➢ **To set up a default DMZ server:**

1. On the WAN Setup screen, select the **Default DMZ Server** check box.
2. Type the IP address.
3. Click **Apply**.

Change the MTU Size

The maximum transmission unit (MTU) is the largest data packet a network device transmits. When one network device communicates across the Internet with another, the data packets travel through many devices along the way. If a device in the data path has a lower MTU setting than the other devices, the data packets have to be split or “fragmented” to accommodate the device with the smallest MTU.

The best MTU setting for On Networks equipment is often just the default value. In some situations, changing the value fixes one problem but causes another. Leave the MTU unchanged unless one of these situations occurs:

- You have problems connecting to your ISP or other Internet service, and the technical support of either the ISP or On Networks recommends changing the MTU setting. These web-based applications might require an MTU change:
  - A secure website that does not open or displays only part of a web page
  - Yahoo email
  - MSN portal
  - America Online’s DSL service
- You use VPN and have severe performance problems.
- You used a program to optimize MTU for performance reasons, and now you have connectivity or performance problems.

Note: An incorrect MTU setting can cause Internet communication problems. For instance, you might not be able to access certain websites, frames within websites, secure login pages, or FTP or POP servers.

If you suspect an MTU problem, a common solution is to change the MTU to 1400. If you are willing to experiment, you can gradually reduce the MTU from the maximum value of 1500

until the problem goes away. The following table describes common MTU sizes and applications.

Table 2. Common MTU sizes

MTU	Application
1500	The largest Ethernet packet size and the default value. This setting is typical for connections that do not use PPPoE or VPN, and is the default value for On Networks modem routers, adapters, and switches.
1492	Used in PPPoE environments.
1472	Maximum size to use for pinging. (Larger packets are fragmented.)
1468	Used in some DHCP environments.
1458	Used in PPPoA environments.
1460	Usable by AOL if you do not have large email attachments, for example.
1436	Used in PPTP environments or with VPN.
1400	Maximum size for AOL DSL.
576	Typical value to connect to dial-up ISPs.

➢ **To change the MTU size:**

1. Select **Advanced > Setup > WAN Setup**.
2. In the MTU Size field, enter a value from 64 to 1500.
3. Click **Apply** to save the settings.

LAN Setup

The LAN Setup screen allows configuration of LAN IP services such as Dynamic Host Configuration Protocol (DHCP) and Routing Information Protocol (RIP).

The modem router is shipped preconfigured to use private IP addresses on the LAN side and to act as a DHCP server. The modem router's default LAN IP configuration is:

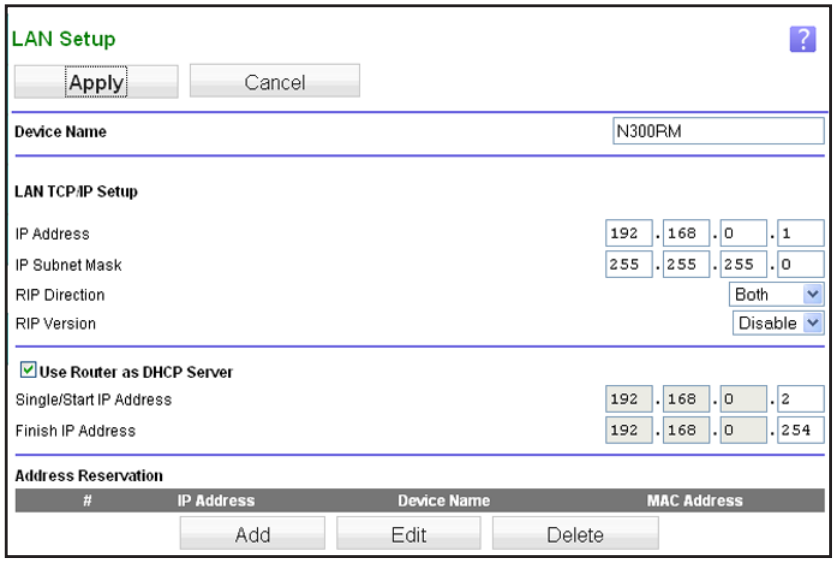
- LAN IP address. **192.168.0.1**
- Subnet mask. **255.255.255.0**

These addresses are part of the designated private address range for use in private networks and are suitable for most applications. If your network requires a different IP addressing scheme, you can change these settings in the LAN Setup screen.

> **Note:** *If you change the LAN IP address of the modem router while connected through the browser, you will be disconnected. You will have to open a new connection to the new IP address and log in again.*

➢ **To change the LAN settings:**

1. Select **Setup > LAN Setup** to display the following screen:



2. Enter the settings that you want to customize. These settings are described in the following section, *LAN TCP/IP Setup*.
3. Click **Apply** to save your changes.

LAN TCP/IP Setup

- **IP Address**. The LAN IP address of the modem router.
- **IP Subnet Mask**. The LAN subnet mask of the modem router. Combined with the IP address, the IP subnet mask allows a device to know which other addresses are local to it, and which have to be reached through a gateway or modem router.
- **RIP Direction**. Router Information Protocol (RIP) allows a router to exchange routing information with other routers. This setting controls how the router sends and receives RIP packets. Both is the default setting. With the Both or Out Only setting, the router broadcasts its routing table periodically. With the Both or In Only setting, the router incorporates the RIP information that it receives.
- **RIP Version**. This setting controls the format and the broadcasting method of the RIP packets that the modem router sends. It recognizes both formats when receiving. By default, the RIP function is disabled.

  RIP-1 is universally supported. It is adequate for most networks, unless you have an unusual network setup.

  RIP-2 carries more information. Both RIP-2B and RIP-2M send the routing data in RIP-2 format. RIP-2B uses subnet broadcasting. RIP-2M uses multicasting.

Use Router as a DHCP Server

This check box is selected by default so that the modem router functions as a Dynamic Host Configuration Protocol (DHCP) server.

- **Starting IP Address**. Specify the start of the range for the pool of IP addresses in the same subnet as the modem router.
- **Ending IP Address**. Specify the end of the range for the pool of IP addresses in the same subnet as the modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer receives the same IP address each time it accesses the modem router's DHCP server. Assign reserved IP addresses to servers that require permanent IP settings.

Use the Modem Router as a DHCP Server

By default, the modem router acts as a DHCP server. The router assigns IP, DNS server, and default gateway addresses to all computers connected to the LAN. The assigned default gateway address is the LAN address of the modem router. The modem router assigns IP addresses to the attached computers from a pool of addresses specified in this screen. Each pool address is tested before it is assigned to avoid duplicate addresses on the LAN. For most applications, the default DHCP and TCP/IP settings of the modem router are satisfactory.

You can specify the pool of IP addresses to be assigned by setting the starting IP address and ending IP address. These addresses should be part of the same IP address subnet as the modem router's LAN IP address. Using the default addressing scheme, define a range between 192.168.0.2 and 192.168.0.254, although you might want to save part of the range for devices with fixed addresses.

The modem router delivers the following parameters to any LAN device that requests DHCP:

- An IP address from the range you have defined
- Subnet mask
- Gateway IP address (the modem router's LAN IP address)
- Primary DNS server (if you entered a primary DNS address in the Basic Settings screen; otherwise, the modem router's LAN IP address)
- Secondary DNS server (if you entered a secondary DNS address in the Basic Settings screen)

To use another device on your network as the DHCP server, or to specify the network settings of all of your computers, clear the **Use Router as DHCP Server** check box and click **Apply**. Otherwise, leave this check box selected. If this service is not enabled and no other DHCP server is available on your network, set your computers' IP addresses manually or they will not be able to access the modem router.

Address Reservation

When you specify a reserved IP address for a computer on the LAN, that computer always receives the same IP address each time it accesses the modem router's DHCP server. Assign reserved IP addresses to computers or servers that require permanent IP settings.

➢ **To reserve an IP address:**

1. In the Address Reservation section of the screen, click the **Add** button.
2. In the IP Address field, type the IP address to assign to the computer or server. (Choose an IP address from the modem router's LAN subnet, such as 192.168.0.x.)
3. Type the MAC address of the computer or server.

   Tip: If the computer is already on your network, you can copy its MAC address from the Attached Devices screen and paste it here.

4. Click **Apply** to enter the reserved address into the table.

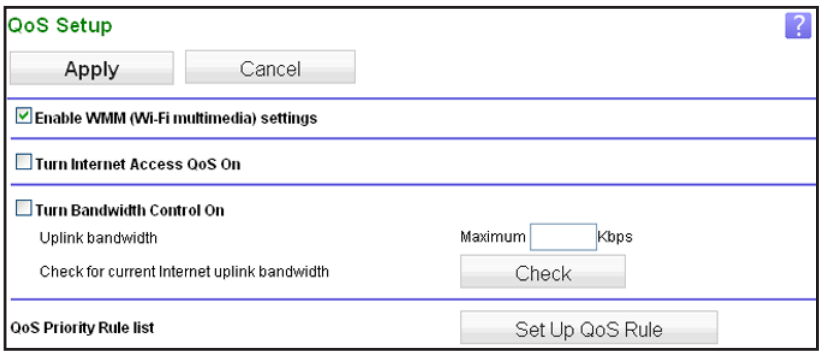
   The reserved address is not assigned until the next time the computer contacts the modem router's DHCP server. Reboot the computer, or access its IP configuration and force a DHCP release and renew.

To edit or delete a reserved address entry, select the radio button next to the reserved address you want to edit or delete. Then click **Edit** or **Delete**.

Quality of Service (QoS) Setup

QoS is an advanced feature that can be used to prioritize some types of traffic ahead of others. The modem router can provide QoS prioritization over the wireless link and on the Internet connection. To configure QoS, use the QoS Setup screen.

Select **Setup > QoS Setup** to display the following screen:



Enable WMM QoS for Wireless Multimedia Applications

The modem router supports Wi-Fi Multimedia Quality of Service (WMM QoS) to prioritize wireless voice and video traffic over the wireless link. WMM QoS provides prioritization of wireless data packets from different applications based on four access categories: voice,

video, best effort, and background. For an application to receive the benefits of WMM QoS, both it and the client running that application have to have WMM enabled. Legacy applications that do not support WMM and applications that do not require QoS, are assigned to the best effort category, which receives a lower priority than voice and video.

WMM QoS is enabled by default. You can disable it in the QoS Setup screen by clearing the **Enable WMM (Wi-Fi Multimedia) settings** check box and clicking **Apply**.

Set Up QoS for Internet Access

You can give prioritized Internet access to the following types of traffic:

- Specific applications
- Specific online games
- Individual Ethernet LAN ports of the modem router
- A specific device by MAC address

To specify prioritization of traffic, create a policy for the type of traffic and add the policy to the QoS Policy table in the QoS Setup screen. For convenience, the QoS Policy table lists many common applications and online games that can benefit from QoS handling.

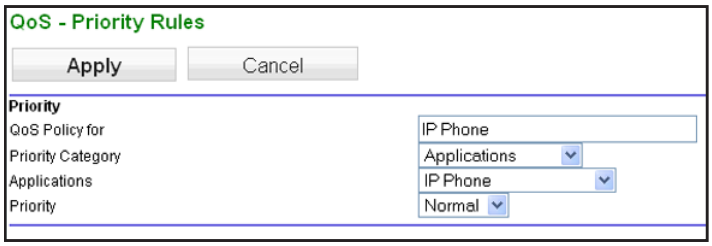
QoS for Applications and Online Gaming

➢ **To create a QoS policy for applications and online games:**

1. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS Rule** button to see the existing priority rules.

You can edit or delete a rule by selecting its radio button and clicking either the **Edit** or **Delete** button. You can also delete all of the rules by simply clicking the **Delete All** button.

3. To add a priority rule, scroll down to the bottom of the QoS Setup screen and click **Add Priority Rule** to display the following screen:



4. In the QoS Policy for field, type the name of the application or game.
5. In the Priority Category list, select either **Applications** or **Online Gaming**. In either case, a list of applications or games displays.
6. You can select an existing item from the list, or you can scroll and select **Add a New Application** or **Add a New Game,** as applicable.

   If you add an entry, the Priority Rules screen expands.

   a. In the QoS Policy for field, enter a name for the new application or game.
   b. In the Connection Type list, select either **TCP, UDP,** or both (**TCP/UDP**). Specify the port number or range of port numbers that the application or game uses.
7. From the Priority list, select the priority for Internet access for this traffic relative to other applications and traffic. The options are Low, Normal, High, and Highest.
8. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.

QoS for a Modem Router LAN Port

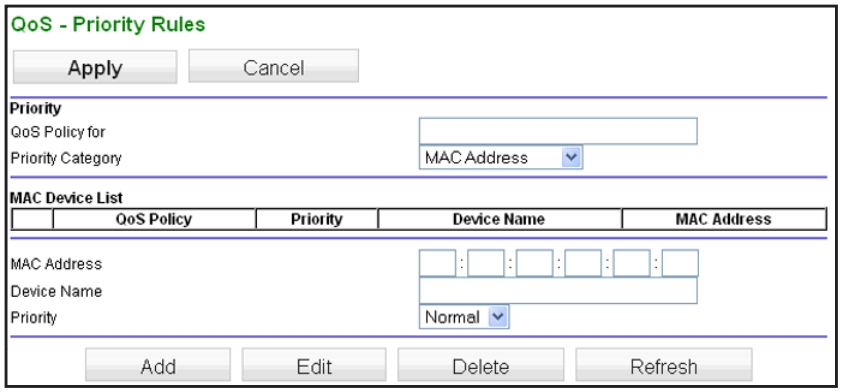
➢ **To create a QoS policy for a device connected to one of the modem router's LAN ports:**

1. Select **QoS Setup** to display the QoS Setup screen. Select the **Turn Internet Access QoS On** check box.
2. Click the **Setup QoS Rule** button.
3. Click the **Add Priority Rule** button.
4. From the Priority Category list, select **Ethernet LAN Port**.
5. From the LAN port list, select the LAN port.
6. From the Priority list, select the priority for Internet access for this port's traffic relative to other applications. The options are Low, Normal, High, and Highest.
7. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
8. In the QoS Setup screen, click **Apply**.

QoS for a MAC Address

➢ **To create a QoS policy for traffic from a specific MAC address:**

1. Select **QoS Setup** and click the **Setup QoS Rule** button. The QoS Setup screen displays.
2. Click **Add Priority Rule**.
3. From the Priority Category list, select **MAC Address**:



4. If the device is the MAC Device List, select its radio button. The information from the MAC Device List populates the policy name, MAC Address, and Device Name fields. If the device is not in the list, click **Refresh**. If it still does not appear, fill in these fields manually.
5. From the Priority list, select the priority for Internet access for this device's traffic relative to other applications and traffic. The options are Low, Normal, High, and Highest.
6. Click **Apply** to save this rule to the QoS Policy list and return to the QoS Setup screen.
7. In the QoS Setup screen, select the **Turn Internet Access QoS On** check box.
8. Click **Apply**.

Edit or Delete an Existing QoS Policy

➢ **To edit or delete a QoS policy:**

1. Select **QoS Setup** to display the QoS Setup screen.
2. Select the radio button next to the QoS policy that you want to edit or delete, and do one of the following:
   - Click **Delete** to remove the QoS policy.
   - Click **Edit** to edit the QoS policy. Follow the instructions in the preceding sections to change the policy settings.
3. Click **Apply** in the QoS Setup screen to save your changes.

Security Settings

4

Security tab (firewall) details

You can customize many of the firewall settings based on your needs. This chapter contains the following sections:

- *Firewall Rules to Control Network Access*
- *Block Internet Sites*
- *Firewall Rules to Control Network Access*
- *Set the Time Zone*
- *Schedule Blocking and Services*
- *Set Up Email Alerts*
- *Port Forwarding and Port Triggering*
- *Set Up Port Forwarding to Local Servers*
- *Set Up Port Triggering*

Firewall Rules to Control Network Access

Your modem router has a firewall that blocks unauthorized access to your wireless network and permits authorized inbound and outbound communications. Authorized communications are established according to inbound and outbound rules. The firewall has the following two default rules. You can create custom rules to further restrict the outbound communications or more widely open the inbound communications:

- **Inbound**. Block all access from outside except responses to requests from the LAN side.
- **Outbound**. Allow all access from the LAN side to the outside.

Inbound Rules (Port Forwarding)

Because the modem router uses Network Address Translation (NAT), your network presents only one IP address to the Internet, and outside users cannot directly address any of your local computers. However, by defining an inbound rule you can make a local server (for example, a web server or game server) visible and available to the Internet.

The rule tells the modem router to direct inbound traffic for a particular service to one local server based on the destination port number. This is also known as port forwarding. Allowing inbound services opens holes in your firewall. Enable only those ports that are necessary for your network. The following are two examples of inbound rules.

Note: Some residential broadband ISP accounts do not let you run server processes (such as a web or FTP server) from your location. Your ISP might periodically check for servers and suspend your account if it discovers any active services at your location. If you are unsure, refer to the acceptable use policy of your ISP.

Outbound Rules (Service Blocking)

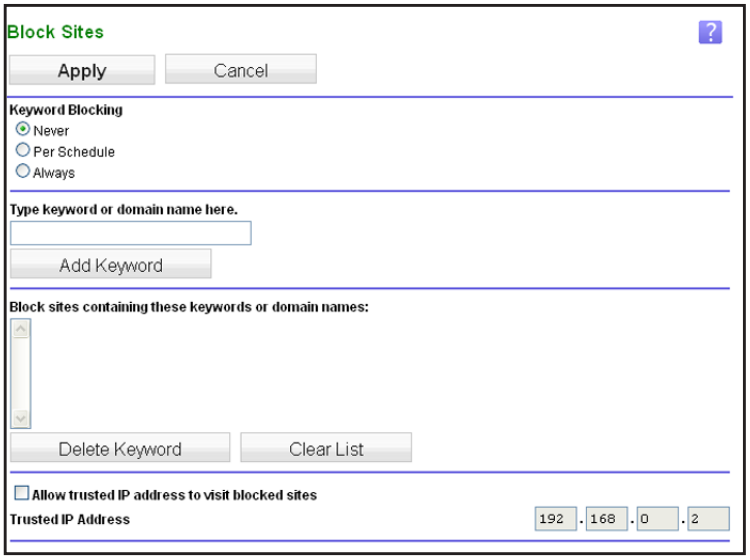
You can block computers on your local network from using certain Internet services. This is called service blocking or port filtering. You can add an outbound rule to block Internet access from a local computer based on the computer, Internet site, time of day, and type of service.

Block Internet Sites

Use keyword blocking to prevent certain types of HTTP traffic from accessing your network. The blocking can be always or according to a schedule.

➢ **To block traffic:**

1. Select **Security > Block Sites**.



2. Select one of the keyword blocking options:
   - **Per Schedule**. Turn on keyword blocking according to the Schedule screen settings.
   - **Always**. Turn on keyword blocking all the time, independent of the Schedule screen.
3. In the keyword field, enter a keyword or domain, click **Add Keyword,** and click **Apply**.

   The keyword list supports up to 32 entries. Here are some sample entries:

   - Specify XXX to block http://www.badstuff.com/xxx.html.
   - Specify .com if you want to allow only sites with domain suffixes such as .edu or .gov.
   - Enter a period (**.**) to block all Internet browsing access.

➢ **To delete keywords:**

1. Select the keyword or domain that you want to delete from the list.
2. Click **Delete Keyword** and click **Apply** to save your changes.

You can exempt one trusted computer from blocking and logging. The computer you exempt has to have a fixed IP address.

➢ **To specify a trusted computer:**

1. In the Trusted IP Address field, enter the IP address.
2. Click **Apply** to save your changes.

Firewall Rules to Control Network Access

The firewall has these default rules.

- **Inbound**. Block all access from outside except responses to requests from the LAN side.
- **Outbound**. Allow all access from the LAN side to the outside.

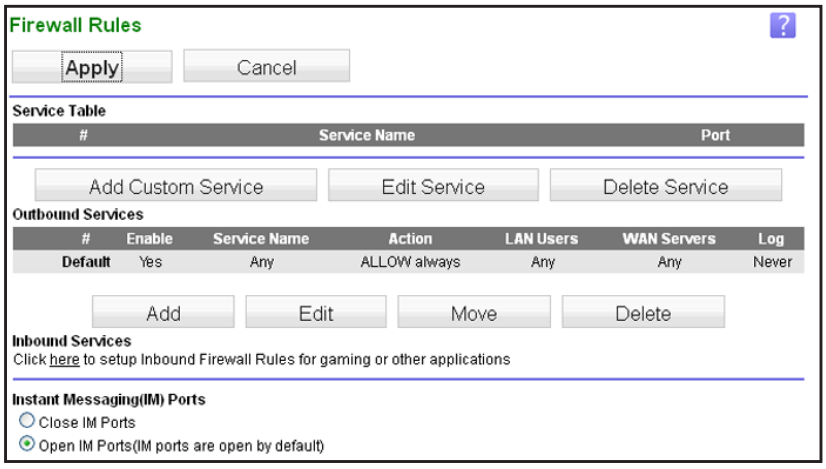
Set Up Firewall Rules

You can create custom rules to further restrict the outbound communications or more widely open the inbound communications. The Firewall Rules screen lets you add custom rules to make exceptions to the default rules. Exceptions can be based on the service or application, source or destination IP addresses, and time of day. You can log traffic that matches or does not match the rule and change the order of rule precedence.

All traffic attempting to pass through the firewall is subjected to the rules in the order shown in the rules table from the top (highest precedence) to the default rules at the bottom. In some cases, the order of precedence is important to determine which communications are allowed into or out of the network.

➢ **To set up firewall rules:**

1. Select **Security > Firewall Rules**.



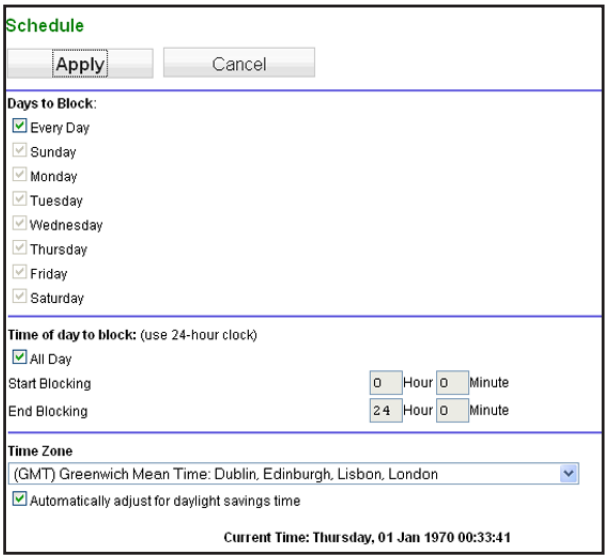
2. To add an outbound rule, click **Add** under Outbound Services. To edit or delete a rule, select its button on the left side and click **Edit** or **Delete**.
3. To change the order of precedence:
   a. Select the button on the left side of the rule and click **Move**.
   b. At the prompt, enter the number of the new position and click **OK**.
4. To open or close instant messaging, select one of the following radio buttons:
   - **Close IM Ports**. Disables instant messaging traffic.
   - **Open IM Ports**. Enables instant messaging traffic. IM ports are open by default.
5. Click **Apply** to save your settings.

Set the Time Zone

The modem router uses the Network Time Protocol (NTP) to obtain the current time and date from one of several network time servers on the Internet.

➢ **To set the time zone:**

1. Select **Security > Schedule**.



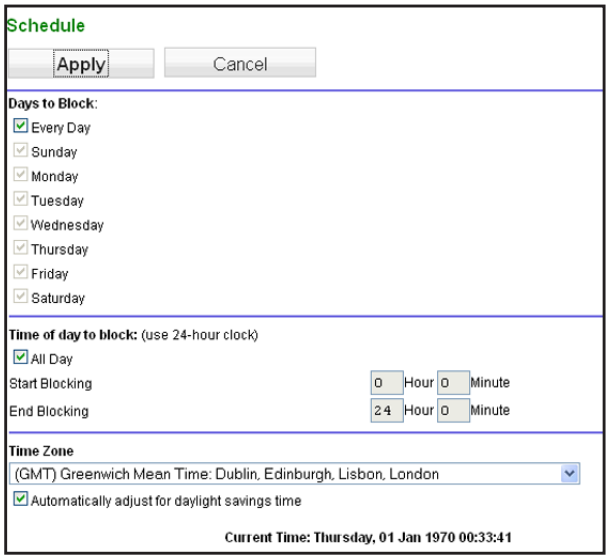
2. Select your time zone. This setting determines the blocking schedule and time-stamping of log entries.
3. If your time zone uses daylight savings time, select the **Automatically adjust for daylight savings time** check box.
4. Click **Apply** to save your settings.

Schedule Blocking and Services

If you enabled service blocking in the Block Services screen or port forwarding in the Ports screen, you can set up a schedule for when blocking occurs or when access is not restricted.

➢ **To schedule services:**

1. Select **Security > Schedule**.



2. To block Internet services based on a schedule, select **Every Day** or select one or more days.
3. If you want to limit access completely for the selected days, select **All Day**. Otherwise, to limit access during certain times for the selected days, enter times in the Start Blocking and End Blocking fields.

   Note: *Enter the values in 24-hour time format. For example, 10:30 a.m. would be 10 hours and 30 minutes, and 10:30 p.m. would be 22 hours and 30 minutes. If you set the start time after the end time, the schedule is effective through midnight the next day.*

4. Click **Apply** to save your settings.

Set Up Email Alerts

To receive logs and alerts by email, provide your email information in the E-mail screen and specify which alerts you want to receive and how often.

Select **Security > Email** to display the following screen:

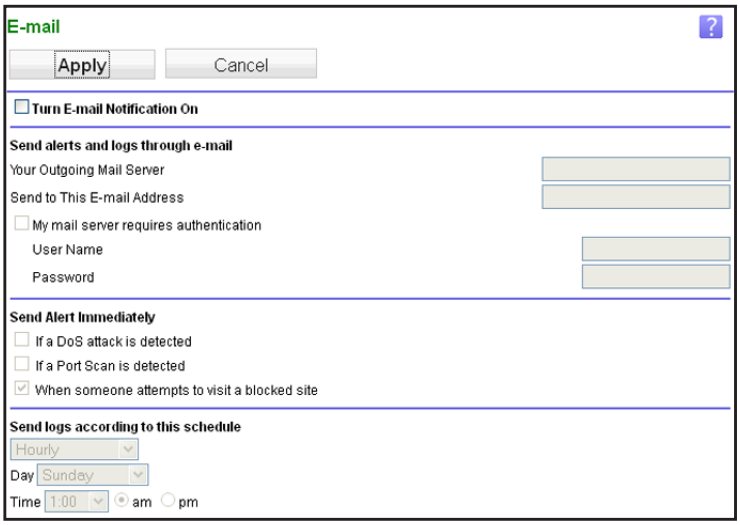


Figure 8. E-Mail screen

- **Turn E-mail Notification On**. Select this check box if you want to receive email logs and alerts from the modem router.
- **Send to This E-mail Address**. Enter the email address where you want logs and alerts sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.
- **Your Outgoing Mail Server**. Enter the name or IP address of your ISP's outgoing (SMTP) mail server (such as mail.myISP.com). You might be able to find this information in the configuration settings of your email program. Enter the email address to which logs and alerts are sent. This email address is also used as the From address. If you leave this field blank, log and alert messages are not sent by email.
- **My mail server requires authentication**. If you use an outgoing mail server that your current ISP provided, you do not need to select this field. If you use an email account that is not provided by your ISP, select this field, and enter the required user name and password information.
- **Send Alerts Immediately**. Select the corresponding check box if you would like immediate notification of a significant security event, such as a known attack, port scan, or attempted access to a blocked site.
- **Send logs according to this schedule**. Specifies how often to send the logs: Hourly, Daily, Weekly, or When Full.
  - **Days**. Specify which day of the week to send the log. This is relevant when the log is sent weekly.

- **Time**. Specify the time of day to send the log. This is relevant when the log is sent daily or weekly.

Note: If the Weekly, Daily, or Hourly option is selected and the log fills up before the specified period, the log is automatically emailed to the specified email address. After the log is sent, it is cleared from the modem router's memory. If the modem router cannot email the log file, the log buffer might fill up. In this case, the modem router overwrites the log and discards its contents.

Port Forwarding and Port Triggering

By default, the modem router blocks inbound traffic from the Internet to your computers except replies to your outbound traffic. You might need to create exceptions to this rule for these purposes:

- To allow remote computers on the Internet to access a server on your local network.
- To allow certain applications and games to work correctly when your router does not recognize their replies.

Your modem router provides two features for creating these exceptions: port forwarding and port triggering. The next sections provide background information to help you understand how port forwarding and port triggering work, and the differences between the two.

Remote Computer Access Basics

When a computer on your network needs to access a computer on the Internet, your computer sends your modem router a message containing the source and destination address and process information. Before forwarding your message to the remote computer, your modem router has to modify the source information and create and track the communication session so that replies can be routed back to your computer.

Here is an example of normal outbound traffic and the resulting inbound responses:

1. You open a browser, and your operating system assigns port number 5678 to this browser session.
2. You type http://www.example.com into the URL field, and your computer creates a web page request message with the following address and port information. The request message is sent to your modem router.

   Source address. Your computer's IP address.

   Source port number. 5678, which is the browser session.

   Destination address. The IP address of www.example.com, which your computer finds by asking a DNS server.

Destination port number. 80, which is the standard port number for a web server process.

3. Your modem router creates an entry in its internal session table describing this communication session between your computer and the web server at www.example.com. Before sending the web page request message to www.example.com, your modem router stores the original information and then modifies the source information in the request message, performing Network Address Translation (NAT):
   - The source address is replaced with your modem router's public IP address. This is necessary because your computer uses a private IP address that is not globally unique and cannot be used on the Internet.
   - The source port number is changed to a number assigned by the modem router, such as 33333. This is necessary because two computers could independently be using the same session number.

   Your modem router then sends this request message through the Internet to the web server at www.example.com.
4. The web server at www.example.com composes a return message with the requested web page data. The return message contains the following address and port information. The web server then sends this reply message to your modem router.

   Source address. The IP address of www.example.com.

   Source port number. 80, which is the standard port number for a web server process.

   Destination address. The public IP address of your modem router.

   Destination port number. 33333.
5. Upon receiving the incoming message, your modem router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the modem router then modifies the message to restore the original address information replaced by NAT. Your modem router sends this reply message to your computer, which displays the web page from www.example.com. The message now contains the following address and port information.

   Source address. The IP address of www.example.com.

   Source port number. 80, which is the standard port number for a web server process.

   Destination address. Your computer's IP address.

   Destination port number. 5678, which is the browser session that made the initial request.
6. When you finish your browser session, your modem router eventually detects a period of inactivity in the communications. Your modem router then removes the session information from its session table, and incoming traffic is no longer accepted on port number 33333.

Port Triggering to Open Incoming Ports

In the preceding example, requests are sent to a remote computer by your modem router from a service port with a particular number. Replies from the remote computer to your modem router are directed to that port. If the remote server sends a reply to a different port, your modem router does not recognize it and discards it. However, some application servers (such as FTP and IRC servers) send replies to multiple ports. Using the port triggering function of your modem router, you can tell the modem router to open additional incoming ports when a particular outgoing port originates a session.

An example is Internet Relay Chat (IRC). Your computer connects to an IRC server at destination port 6667. The IRC server not only responds to your originating source port, but also sends an “identify” message to your computer on port 113. Using port triggering, you can tell the modem router, “When you initiate a session with destination port 6667, you have to also allow incoming traffic on port 113 to reach the originating computer.” Using steps similar to the preceding example, the following sequence shows the effects of the port triggering rule you have defined:

1. You open an IRC client program to start a chat session on your computer.
2. Your IRC client composes a request message to an IRC server using a destination port number of 6667, the standard port number for an IRC server process. Your computer then sends this request message to your modem router.
3. Your modem router creates an entry in its internal session table describing this communication session between your computer and the IRC server. Your modem router stores the original information, performs Network Address Translation (NAT) on the source address and port, and sends this request message through the Internet to the IRC server.
4. Noting your port triggering rule and having observed the destination port number of 6667, your modem router creates an additional session entry to send any incoming port 113 traffic to your computer.
5. The IRC server sends a return message to your modem router using the NAT-assigned source port (as in the previous example, say port 33333) as the destination port. The IRC server also sends an “identify” message to your modem router with destination port 113.
6. Upon receiving the incoming message to destination port 33333, your modem router checks its session table to determine whether there is an active session for port number 33333. Finding an active session, the modem router restores the original address information replaced by NAT and sends this reply message to your computer.
7. Upon receiving the incoming message to destination port 113, your modem router checks its session table and learns that there is an active session for port 113, associated with your computer. The modem router replaces the message’s destination IP address with your computer’s IP address and forwards the message to your computer.
8. When you finish your chat session, your modem router eventually senses a period of inactivity in the communications. The modem router then removes the session information from its session table, and incoming traffic is no longer accepted on port numbers 33333 or 113.

To configure port triggering, you need to know which inbound ports the application needs. Also, you need to know the number of the outbound port that will trigger the opening of the

inbound ports. You can usually determine this information by contacting the publisher of the application or user groups or newsgroups.

Note: Only one computer at a time can use the triggered application.

Port Forwarding to Permit External Host Communications

In both of the preceding examples, your computer initiates an application session with a server computer on the Internet. However, you might need to allow a client computer on the Internet to initiate a connection to a server computer on your network. Normally, your modem router ignores any inbound traffic that is not a response to your own outbound traffic. You can configure exceptions to this default rule by using the port forwarding feature.

A typical application of port forwarding can be shown by reversing the client-server relationship from the previous web server example. In this case, a remote computer's browser needs to access a web server running on a computer in your local network. Using port forwarding, you can tell the modem router, "When you receive incoming traffic on port 80 (the standard port number for a web server process), forward it to the local computer at 192.168.0.123." The following sequence shows the effects of the port forwarding rule you have defined:

1. A person using a remote computer opens a browser and requests a web page from www.example.com, which resolves to the public IP address of your modem router. The remote computer composes a web page request message with the following destination information:

   Destination address. The IP address of www.example.com, which is the address of your modem router.

   Destination port number. 80, which is the standard port number for a web server process.

   The remote computer then sends this request message through the Internet to your modem router.

2. Your modem router receives the request message and looks in its rules table for any rules covering the disposition of incoming port 80 traffic. Your port forwarding rule specifies that incoming port 80 traffic is forwarded to local IP address 192.168.0.123. Therefore, your modem router modifies the destination information in the request message:

   The destination address is replaced with 192.168.0.123.

   Your modem router then sends this request message to your local network.

3. Your web server at 192.168.0.123 receives the request and composes a return message with the requested web page data. Your web server then sends this reply message to your modem router.
4. Your modem router performs NAT on the source IP address, and sends this request message through the Internet to the remote computer, which displays the web page from www.example.com.

To configure port forwarding, you need to know which inbound ports the application needs. You usually can determine this information by contacting the publisher of the application or the relevant user groups and newsgroups.

How Port Forwarding Differs from Port Triggering

The following points summarize the differences between port forwarding and port triggering:

- Port triggering can be used by any computer on your network, although only one computer can use it at a time.
- Port forwarding is configured for a single computer on your network.
- Port triggering does not require that you know the computer's IP address in advance. The IP address is captured automatically.
- Port forwarding requires that you specify the computer's IP address during configuration, and the IP address can never change.
- Port triggering requires specific outbound traffic to open the inbound ports, and the triggered ports are closed after a period of no activity.
- Port forwarding is always active and does not need to be triggered.

Set Up Port Forwarding to Local Servers

Using the port forwarding feature, you can allow certain types of incoming traffic to reach servers on your local network. For example, you might want to make a local web server, FTP server, or game server visible and available to the Internet.

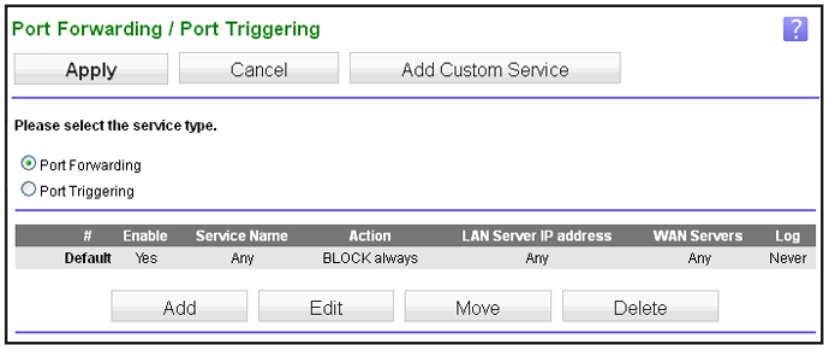
Use the Port Forwarding/Port Triggering screen to configure the modem router to forward specific incoming protocols to computers on your local network. In addition to servers for specific applications, you can also specify a default DMZ server to which all other incoming protocols are forwarded.

Before starting, determine which type of service, application, or game you want to provide. Find out the local IP address of the computer that will provide the service. The server computer has to always have the same IP address.

➢ **To set up port forwarding:**

Tip: To ensure that your server computer always has the same IP address, use the reserved IP address feature of your modem router.

1. Select **Advanced > Port Forwarding/Port Triggering** to display the following screen:



   Port Forwarding is selected as the service type.

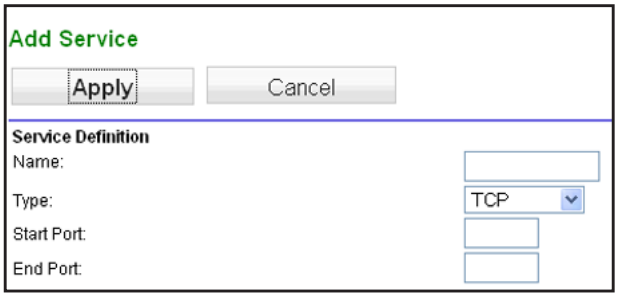
2. From the Service Name list, select the service or game that you will host on your network. If the service does not appear in the list, see *Add a Custom Service* on page 55.
3. Click **Add**. The service appears in the list in the screen.

Add a Custom Service

To define a service, game, or application that does not appear in the Service Name list, first determine which port number or range of numbers the application uses. You can usually get this information by contacting the publisher of the application or user groups or newsgroups.

➢ **To add a custom service:**

1. Select **Advanced > Port Forwarding/Port Triggering**.
2. Select **Port Forwarding** as the service type.
3. Click the **Add Custom Service** button to display the following screen:



4. In the Name field, enter a descriptive name.
5. In the list, select the protocol. If you are unsure, select **TCP/UDP**.
6. In the Start Port field, enter the beginning port number.
   - If the application uses a single port, enter the same port number in the End Port field.
   - If the application uses a range of ports, enter the ending port number of the range in the End Port field.
7. Click **Apply**. The service appears in the list in the Port Forwarding/Port Triggering screen.

Edit or Delete a Port Forwarding Entry

➢ **To edit or delete a port forwarding entry:**

1. In the table, select the radio button next to the service name.
2. Click **Edit Service** or **Delete Service**.

Application Example: Making a Local Web Server Public

If you host a web server on your local network, you can use port forwarding to allow web requests from anyone on the Internet to reach your web server.

➢ **To make a local web server public:**

1. Assign your web server either a fixed IP address or a dynamic IP address using DHCP address reservation. In this example, your modem router always gives your web server an IP address of 192.168.0.33.
2. In the Port Forwarding/Port Triggering screen, configure the modem router to forward the HTTP service to the local address of your web server at **192.168.0.33**. HTTP (port 80) is the standard protocol for web servers.
3. (Optional.) Register a host name with a Dynamic DNS service, and configure your modem router to use the name as described in *Dynamic DNS* on page 75. To access your web server from the Internet, a remote user has to know the IP address that your ISP assigned. However, if you use a Dynamic DNS service, the remote user can reach your server by a user-friendly Internet name, such as mynetwork.dyndns.org.

Set Up Port Triggering

Port triggering is a dynamic extension of port forwarding that is useful in these cases:

- More than one local computer needs port forwarding for the same application (but not simultaneously).
- An application needs to open incoming ports that are different from the outgoing port.

When port triggering is enabled, the modem router monitors outbound traffic looking for a specified outbound “trigger” port. When the modem router detects outbound traffic on that port, it remembers the IP address of the local computer that sent the data. The modem router then temporarily opens the specified incoming port or ports, and forwards incoming traffic on the triggered ports to the triggering computer.

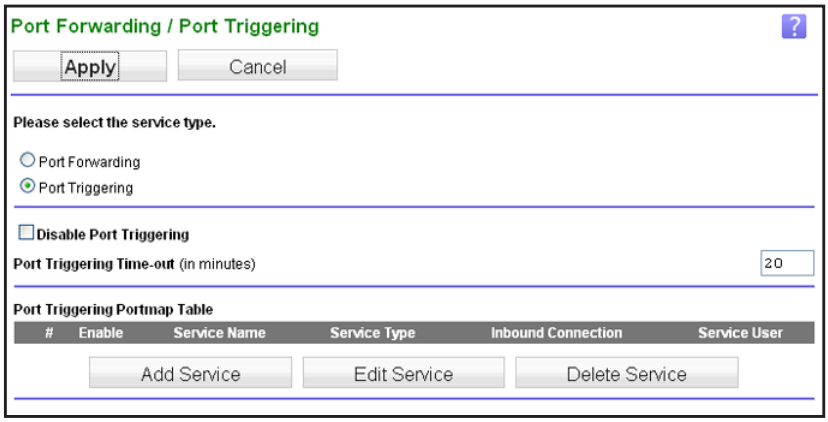
Port forwarding creates a static mapping of a port number or range to a single local computer. Port triggering can dynamically open ports to any computer that needs them and can close the ports when they are no longer needed.

Note: If you use applications such as multiplayer gaming, peer-to-peer connections, real-time communications such as instant messaging, or remote assistance (a feature in Windows XP), you should also enable Universal Plug and Play (UPnP) according to the instructions in *Universal Plug and Play* on page 79.

To set up port triggering, you need to know which inbound ports the application needs and the number of the outbound port that will trigger the opening of the inbound ports. You can usually get this information by contacting the publisher of the application or user groups or newsgroups.

➢ **To set up port triggering:**

1. Select **Advanced > Port Forwarding/Port Triggering**.
2. Select the **Port Triggering** radio button to display the port triggering information.



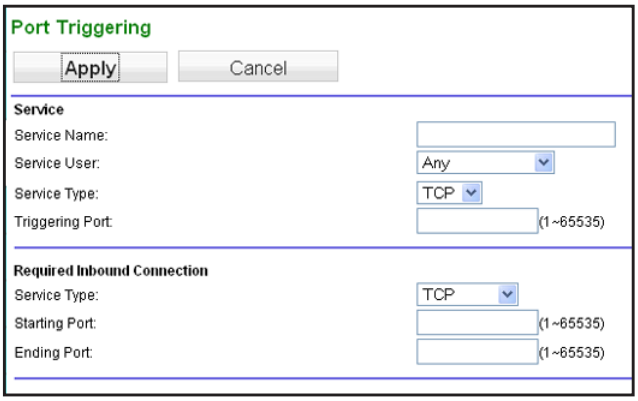
3. Clear the **Disable Port Triggering** check box if it is selected.

   Note: *If the Disable Port Triggering check box is selected after you configure port triggering, port triggering is disabled. However, any port triggering configuration information you added to the modem router is retained even though it is not used.*

4. In the Port Triggering Time-out field, enter a value up to 9999 minutes.

   This value controls the inactivity timer for the designated inbound ports. The inbound ports close when the inactivity time expires. This is required because the modem router cannot be sure when the application has terminated.

5. Click **Add Service** to display the following screen:



6. In the Service Name field, type a descriptive service name.
7. In the Service User list, select **Any** (the default) to allow this service to be used by any computer on the Internet. Otherwise, select **Single address** and enter the IP address of one computer to restrict the service to a particular computer.
8. Select the service type, either **TCP** or **UDP** or both (**TCP/UDP**). If you are not sure, select TCP/UDP.
9. In the Triggering Port field, enter the number of the outbound traffic port that will cause the inbound ports to be opened.
10. Enter the inbound connection port information in the Connection Type, Starting Port, and Ending Port fields.
11. Click **Apply**. The service appears in the Port Triggering Portmap table.

Network Management

5

Management tab options

This chapter contains the following sections:

- *Upgrade the Modem Router Firmware*
- *Check for Firmware Upgrades*
- *Backup Settings*
- *Change Password*
- *View Router Status*
- *View Attached Devices*
- *Logs*

Upgrade the Modem Router Firmware

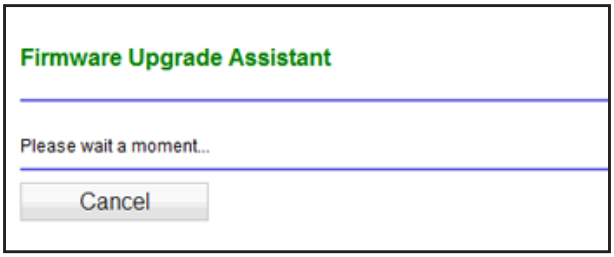
The modem router firmware (routing software) is stored in flash memory. By default, when you log in to your modem router, it checks the On Networks website for new firmware and alerts you if there is a newer version.

WARNING:

When uploading firmware to the modem router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

Automatic Firmware Check

When automatic firmware checking is on, the modem router performs the check and notifies you if an upgrade is available or not.



- **To check the firmware automatically:**

1. Click **Yes** to allow the modem router to download and install the new firmware. The upgrade process could take a few minutes. When the upload is complete, your modem router restarts.
2. Go to the N300RM support page and read the new firmware release notes to determine whether you need to reconfigure the modem router after upgrading.

Note: If you get a “Firmware needs to be reloaded” message, it means that a problem has been detected with the modem router’s firmware. Follow the prompts to correct the problem.

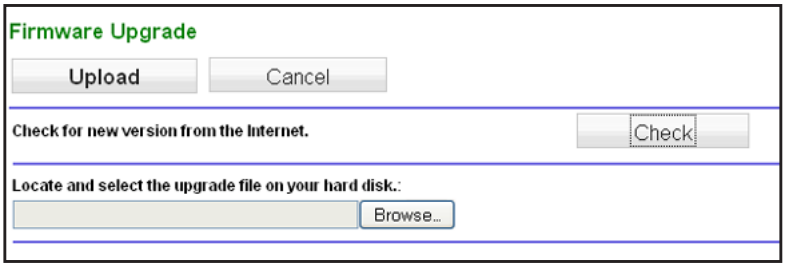
Check for Firmware Upgrades

You can use the Firmware Upgrade screen to manually check the On Networks website for newer versions of firmware for your product.

WARNING:

When uploading firmware to the modem router, *do not* interrupt the web browser by closing the window, clicking a link, or loading a new page. If the browser is interrupted, it could corrupt the firmware.

1. Select **Management > Firmware Update**.



2. Click **Browse**, and locate the firmware image that you downloaded to your computer (the file ends in .img or .chk).
3. Click **Upload** to send the firmware to the router.

   When the upload is complete, your modem router restarts. The upgrade process typically takes about 1 minute. Read the new firmware release notes to determine whether you need to reconfigure the modem router after upgrading.

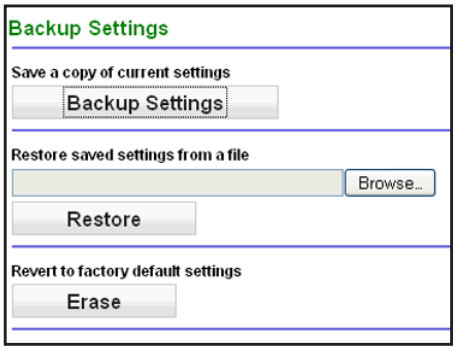
Backup Settings

The modem router configuration settings are stored in a configuration file (*.cfg). This file can be backed up to your computer, restored, or used to revert to factory default settings.

Back Up

➢ **To back up the configuration file:**

1. Select **Management > Backup Settings** to display the following screen:



2. Click **Save** to save a copy of the current settings.
3. Choose a location to store the .cfg file that is on a computer on your network.

Restore

➢ **To restore the configuration file:**

1. Enter the full path to the file on your network or click the **Browse** button to find the file.
2. When you have located the .cfg file, click the **Restore** button to upload the file to the modem router.

   Upon completion, the modem router reboots.

Erase

Click the **Erase** button to reset the modem router to its factory default settings. Erase sets the password to **password** and the LAN IP address to **192.168.0.1**, and enables the modem router's DHCP.

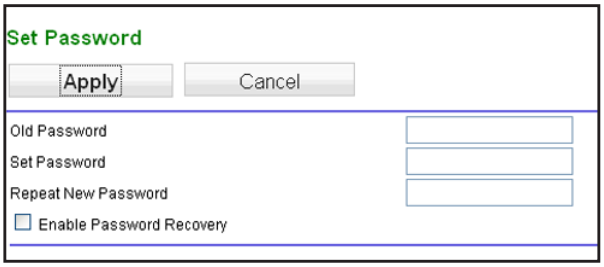
Change Password

For security reasons, the modem router has its own user name and password that default to admin and password. You can and should change these to a secure user name and password that are easy to remember. The ideal password contains no dictionary words from any language and is a mixture of upper case and lower case letters, numbers, and symbols. It can be up to 30 characters.

The modem router user name and password are not the same as the user name and password for logging in to your Internet connection.

➢ **To change the password:**

1. Select **Management > Set Password** to display the following screen.



2. Enter the old password.
3. Enter the new password twice.
4. Click **Apply** to save your changes.

After changing the password, you are required to log in again to continue the configuration. If you have backed up the modem router settings previously, you should do a new backup so that the saved settings file includes the new password. See *Back Up* on page 62 for information about backing up your network configuration.

Password Recovery

On Networks recommends that you enable password recovery if you change the password for the router's user name of admin. Then if the password is forgotten, you can recover it. This recovery process is supported in Internet Explorer, Firefox, and Chrome browsers, but not in the Safari browser.

➢ **To set up password recovery:**

1. Select the **Enable Password Recovery** check box.
2. Select two security questions, and provide answers to them.
3. Click **Apply** to save your changes.

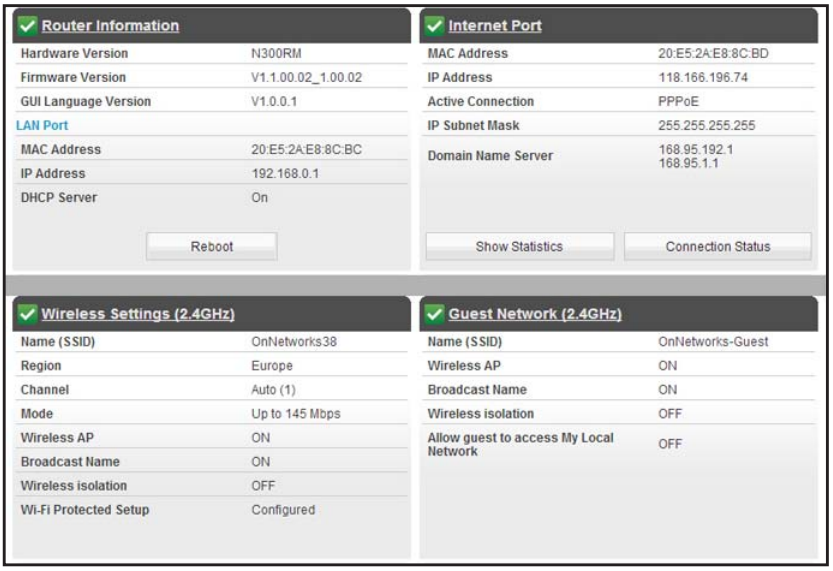
When you use your browser to access the router, the login window displays. If password recovery is enabled, when you click Cancel, the password recovery process starts. You can then enter the saved answers to the security questions to recover the password.

View Router Status

The Router Status screen provides status and usage information.

➢ **To view the router status:**

Select **Management > Router Status** to display this screen.



The following information is displayed:

Router Information

Hardware and Firmware Version. The model of the hardware and the currently running firmware version.

GUI Language Version. The currently selected language.

LAN Port (Local Ports)

MAC Address. The modem router LAN port Ethernet MAC address.

IP Address. The modem router LAN port IP address. The default is 192.168.0.1.

DHCP. If Off, the modem router does not assign IP addresses to PCs on the LAN. If On, the modem router does assign IP addresses to computers on the LAN.

Internet Port Settings

MAC Address. The Ethernet MAC address of the DSL port.

IP Address. The Internet port IP address. If no address is shown, the modem router cannot connect to the Internet.

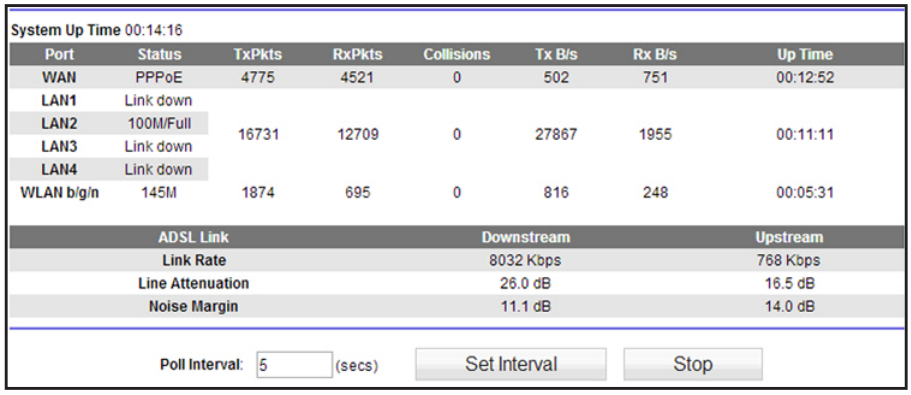
Active Connection. The value depends on your ISP.

IP Subnet Mask. The Internet port IP subnet mask.

Domain Name Server. The modem router DNS server IP addresses. These addresses are usually obtained dynamically from the ISP.

Show Statistics

Click the **Show Statistics** button on the Router Status screen to display a screen similar to the following:



System Up Time 00:14:16

Port	Status	TxPkts	RxPkts	Collisions	Tx B/s	Rx B/s	Up Time
WAN	PPPoE	4775	4521	0	502	751	00:12:52
LAN1	Link down	16731	12709	0	27867	1955	00:11:11
LAN2	100M/Full						
LAN3	Link down						
LAN4	Link down						
WLAN b/g/n	145M	1874	695	0	816	248	00:05:31

ADSL Link	Downstream	Upstream
Link Rate	8032 Kbps	768 Kbps
Line Attenuation	26.0 dB	16.5 dB
Noise Margin	11.1 dB	14.0 dB

Poll Interval: 5 (secs) Set Interval Stop

Port

The statistics for the WAN (Internet), LAN (local), and wireless LAN (WLAN) ports. For each port, the screen displays the following:

- **Status**. The link status of the port.
- **TxPkts**. The number of packets transmitted since reset or manual clear.
- **RxPkts**. The number of packets received since reset or manual clear.
- **Collisions**. The number of collisions since reset or manual clear.
- **Tx B/s**. The current line utilization—percentage of current bandwidth used.
- **Rx B/s**. The average line utilization.
- **Up Time**. The time elapsed since the last power cycle or reset.

ADSL Link Downstream or Upstream

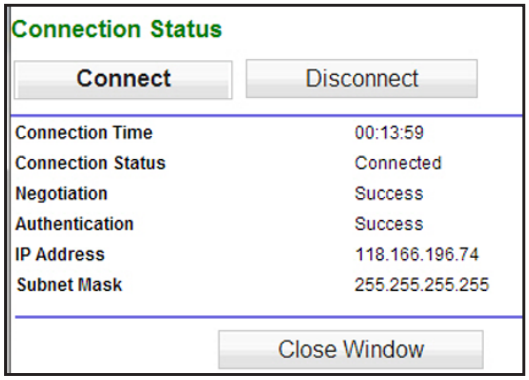
The statistics for the upstream and downstream DSL link. These statistics are of interest to your technical support representative if you have problems obtaining or maintaining a connection.

- **Connection Speed**. Typically, the downstream speed is faster than the upstream speed.
- **Line Attenuation**. The line attenuation increases the farther you are physically located from your ISP’s facilities.
- **Noise Margin**. The signal-to-noise ratio, which is a measure of the quality of the signal on the line.

- **Poll Interval**. The interval at which the statistics are updated in this window. Click the **Stop** button to freeze the display.

Connection Status

In the Router Status screen, click the **Connection Status** button:



- **Connection Time**. The time elapsed since the last connection to the Internet through the Internet port.
- **Connection Status**. The connection status.
- **Negotiation**. On or Off.
- **Authentication**. On or Off.
- **IP Address**. The IP address assigned to the WAN port by the ISP.
- **Subnet Mask**. The network mask assigned to the WAN port by the ISP.

Wireless Settings and Guest Network (2.4GHz)

See *Wireless Setup* on page 30 for a more detailed description of these settings.

Name (SSID). The Wi-Fi network name (service set ID) for the wireless network.

Region. The country where the unit is set up for use.

Channel. The current channel, which determines the operating frequency.

Mode. The current Mbps setting.

Wireless AP. Indicates if the access point feature is enabled. If disabled, the Wireless LED on the front panel is off.

Broadcast Name. Indicates if the modem router is configured to broadcast its SSID.

Wireless Isolation. If this is on, wireless computers or devices that join the network can use the Internet but cannot access each other or access Ethernet devices on the network

Wi-Fi Protected Setup. Shows whether WPS is configured on this network.

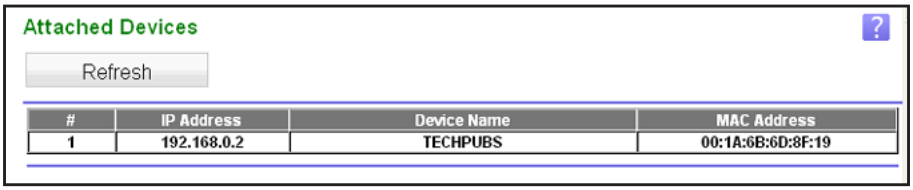
Allow guest to access My Local Network. If this is on, then people who use your guest network can access equipment on your network, not just the Internet connection.

View Attached Devices

The Attached Devices screen shows all IP devices that the modem router has discovered on the local network.

- **To view attached devices:**

  Select **Management > Attached Devices**.



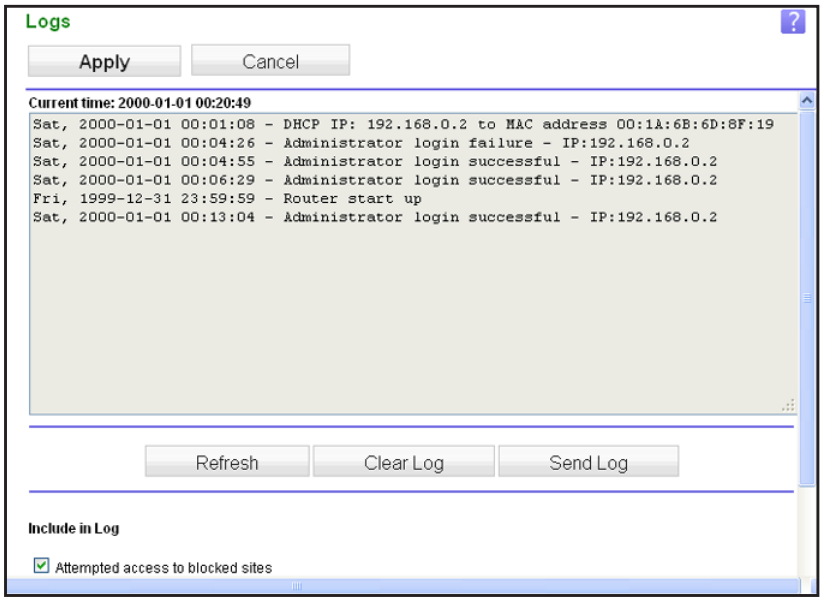
For each device, the table shows the IP address, the device name if available, and the Ethernet MAC address. If the modem router is rebooted, the table data is lost until the modem router rediscovers the devices. To force the modem router to look for attached devices, click the **Refresh** button.

Logs

The modem router logs security-related events such as denied incoming service requests, hacker probes, and administrator logins. If you enable content filtering in the Block Sites screen, the Logs screen show you when someone on your network tries to access a blocked site. If you enable email notification, you will receive these logs in an email message.

- **To view the log:**

  Select **Management > Logs**. A screen similar to the following displays:



The Include in Log check boxes allow you to select which events are logged. You can write the logs to a computer running a syslog program. To activate this feature, select **Broadcast on LAN**, or enter the IP address of the server where the syslog file will be written. The security log entries include the following information:

- **Date and time**. The date and time the log entry was recorded.
- **Description or action**. The type of event and what action was taken, if any.
- **Source IP**. The IP address of the initiating device for this log entry.
- **Source port and interface**. The service port number of the initiating device, and whether it originated from the LAN or WAN.
- **Destination**. The name or IP address of the destination device or website.
- **Destination port and interface**. The service port number of the destination device, and whether it is on the LAN or WAN.

Advanced Settings

6

Advanced tab settings for unique situations

This chapter describes the advanced features of your modem router. The information is for readers with advanced networking knowledge who want to set the modem router up for unique situations such as when remote access from the Internet by IP or domain name is needed.

> **Note:** For information about port forwarding and port triggering, see *Chapter 4, Security Settings*.

This chapter includes the following sections:

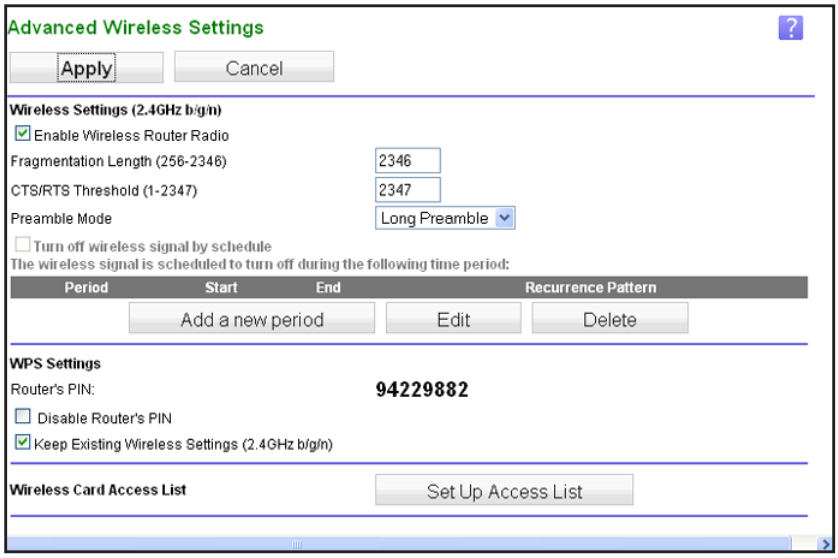
- *Advanced Wireless Settings*
- *Wireless Repeating (WDS)*
- *Dynamic DNS*
- *Static Routes*
- *Remote Management*
- *Universal Plug and Play*
- *Change the Device Mode*

Advanced Wireless Settings

By default, the modem router is set up with wireless settings that work in most situations. You can use this screen to control the wireless router radio and select advanced settings that specifically fit your environment.

➢ **To view or change the advanced wireless settings:**

Select **Advanced > Wireless Settings** to display the following screen:



The following settings are available in this screen:

Enable Wireless Router Radio. You can completely turn off the wireless portion of the wireless modem router by clearing this check box. Select this check box again to enable the wireless portion of the modem router. When the wireless radio is disabled, other members of your household can use the modem router by connecting their computers to the modem router with an Ethernet cable.

> **Note:** The Fragmentation Length, CTS/RTS Threshold, and Preamble Mode options are reserved for wireless testing and advanced configuration only. Do not change these settings.

Turn off wireless signal by schedule. You can use this feature to turn off the wireless signal from your modem router at times when you do not need a wireless connection. For instance, you could turn it off for the weekend if you leave town.

WPS Settings.You can add WPS devices to your network.

Wireless Card Access List. Click the **Set Up Access List** button display the Wireless Card Access List screen. You can restrict access to your network to specific devices based on their MAC address.

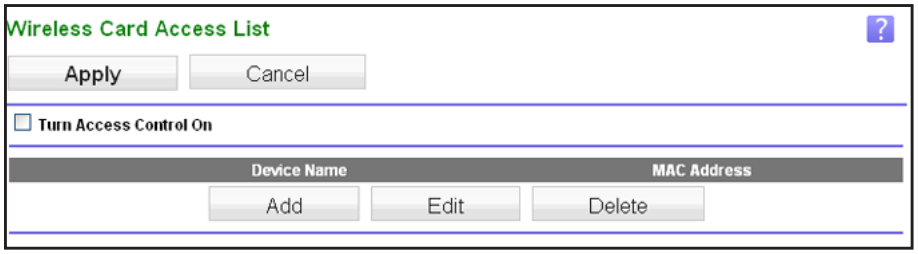
Restrict Wireless Access by MAC Address

You can set up a list of computers and wireless devices that are allowed to join the wireless network. This list is based on the unique MAC address of each computer and device.

Each network device has a MAC address, which is a unique 12-character physical address, containing the hexadecimal characters 0–9, a–f, or A–F only, and separated by colons (for example, 00:09:AB:CD:EF:01). Typically, the MAC address is on the label of the wireless card or network interface device. If you do not have access to the label, you can display the MAC address using the network configuration utilities of the computer. You might also find the MAC addresses in the Attached Devices screen.

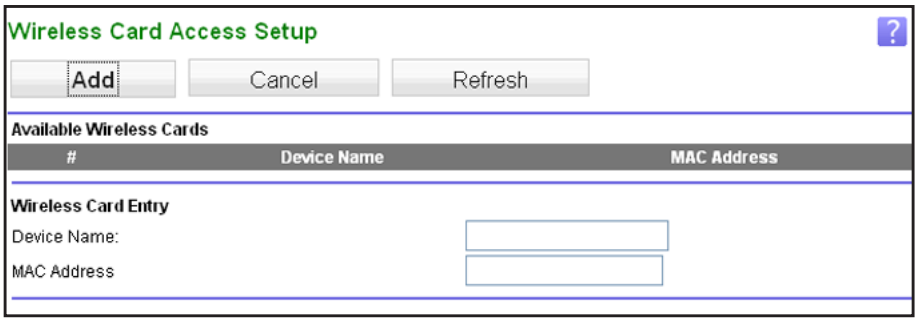
➢ **To restrict access based on MAC addresses:**

1. Select **Advanced > Wireless Setting** and click **Set Up Access List** to display the Wireless Card Access List screen.



2. Click **Add** to add a wireless device to the wireless access control list.

   The Wireless Card Access Setup screen opens and displays a list of currently active wireless cards and their Ethernet MAC addresses.



3. If the computer or device you want is in the Available Wireless Cards list, select that radio button; otherwise, type a name and the MAC address. You can usually find the MAC address on the bottom of the wireless device.

   Tip: You can copy and paste the MAC addresses from the router's Attached Devices screen into the MAC Address field of this screen. To do this, use each wireless computer to join the wireless network. The computer should then appear in the Attached Devices screen.

4. Click **Add** to add this wireless device to the Wireless Card Access List. The screen changes back to the list screen.
5. Add each computer or device you want to allow to connect wirelessly.
6. Select the **Turn Access Control On** check box.
7. Click **Apply**.

Wireless Repeating (WDS)

You can set the modem router up to be used as a wireless access point (AP). Doing this enables the modem router to act as a wireless repeater. A wireless repeater connects to another wireless modem router as a client where the network to which it connects becomes the ISP service.

Wireless repeating is a type of Wireless Distribution System (WDS). A WDS allows a wireless network to be expanded through multiple access points instead of using a wired backbone to link them. The following figure shows a wireless repeating scenario.

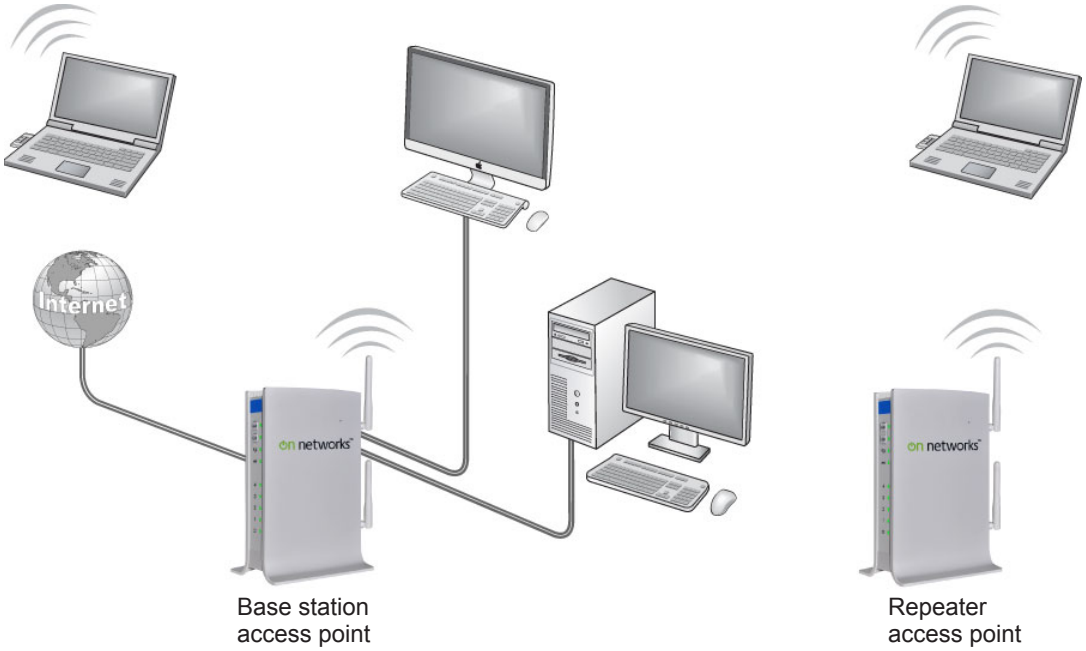


Figure 9. Wireless repeating scenario

If you use the wireless repeating function, you need to select either WEP or None as a security option in the Wireless Settings screen. The WEP option displays only if you select the wireless mode Up to 54 Mbps in the Wireless Settings screen.

Wireless base station. The modem router acts as the parent access point by bridging traffic to and from the child repeater access point. The base station also handles wireless and wired local computers. To configure this mode, you have to know the MAC addresses of the child repeater access point.

Wireless repeater. The modem router sends all traffic from its local wireless or wired computers to a remote access point. To configure this mode, you have to know the MAC address of the remote parent access point.

The modem router is always in dual-band concurrent mode, unless you turn off one radio. If you enable the wireless repeater in either radio band, the wireless base station or wireless repeater cannot be enabled in the other radio band. However, if you enable the wireless base station in either radio band and use the other radio band as a wireless modem router or wireless base station, dual-band concurrent mode is not affected.

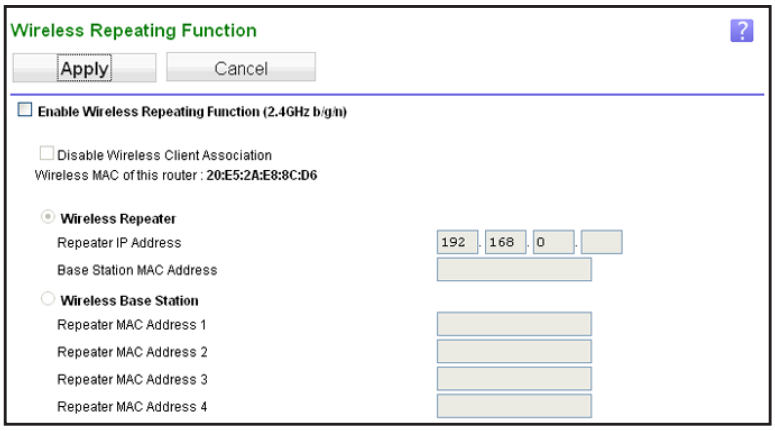
For you to set up a wireless network with WDS, both access points have to meet the following conditions:

- Both access points have to use the same SSID, wireless channel, and encryption mode.
- Both access points have to be on the same LAN IP subnet. That is, all the access point LAN IP addresses are in the same network.
- All LAN devices (wired and wireless computers) are configured to operate in the same LAN network address range as the access points.

Wireless Repeating

➢ **To view or change the wireless repeating settings:**

Select **Advanced > Wireless Repeating Function**.



The following settings are available in this screen:

- **Enable Wireless Repeating Function**. Select this check box to use the wireless repeating function.
- **Disable Wireless Client Association**. If your modem router is the repeater, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.
  - If you are setting up a point-to-point bridge, select this check box.
  - If you want all client traffic to go through the other access point (repeater with wireless client association), leave this check box cleared.

- **Wireless MAC of this router**. This field displays the MAC address for your modem router for your reference. You will need to enter this MAC address in the corresponding Wireless Repeating Function screen of the other access point you are using.
- **Wireless Repeater**. If your modem router is the repeater, select this radio button.

  Repeater IP Address. If your modem router is the repeater, enter the IP address of the other access point.

  Base Station MAC Address. If your modem router is the repeater, enter the MAC address for the access point that is the base station.
- **Wireless Base Station**. If your modem router is the base station, select this radio button.

  Disable Wireless Client Association. If your modem router is the base station, selecting this check box means that wireless clients cannot associate with it. Only LAN client associations are allowed.

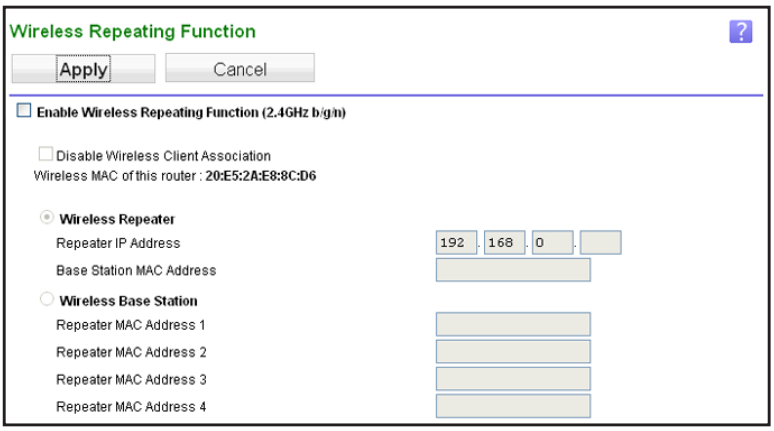
  Repeater MAC Address (1 through 4). If your modem router is the base station, it can act as the “parent” of up to 4 other access points. Enter the MAC addresses of the other access points in these fields.

Set Up the Base Station

The wireless repeating function works only in hub and spoke mode. The units cannot be daisy-chained. You have to know the wireless settings for both units. You have to know the MAC address of the remote unit. First, set up the base station and then set up the repeater.

➢ **To set up the base station:**

1. Set up both units with the same wireless settings (SSID, mode, channel, and security). The wireless security option has to be set to None or WEP.
2. Select **Advanced > Wireless Repeating Function**.



3. Select the **Enable Wireless Repeating Function** check box and select the **Wireless Base Station** radio button.
4. Enter the MAC address for one or more repeater units.
5. Click **Apply** to save your changes.

Set Up a Repeater Unit

Use a wired Ethernet connection to set up the repeater unit to avoid conflicts with the wireless connection to the base station.

> **Note:** If you are using the N300RM base station with a different router product as the repeater, you might need to change additional configuration settings. In particular, you should disable the DHCP server function on the wireless repeater AP.

➢ **To configure the modem router as a repeater unit:**

1. Log in to the modem router that will be the repeater.
2. Select **Basic > Wireless Settings** and verify that the wireless settings match the base unit exactly. The wireless security option has to be set to **WEP** or **None**.
3. Select **Advanced > Wireless Repeating Function**.
4. Select the **Enable Wireless Repeating Function** check box and the **Wireless Repeater** radio button.
5. Fill in the Repeater IP Address field. This IP address has to be in the same subnet as the base station, but different from the LAN IP address of the base station.
6. Click **Apply** to save your changes.
7. Verify connectivity across the LANs.

   A computer on any wireless or wired LAN segment of the modem router should be able to connect to the Internet or share files and printers with any other wireless or wired computer or server connected to the other access point.

Dynamic DNS

If your Internet service provider (ISP) gave you a permanently assigned IP address, you can register a domain name and have that name linked with your IP address by public Domain Name Servers (DNS). Most Internet accounts use dynamically assigned IP addresses. You do not know in advance what your IP address will be, and the address can change frequently. In this case, you can use a commercial Dynamic DNS service. This type of service lets you register your domain to their IP address and forwards traffic directed at your domain to your frequently changing IP address.

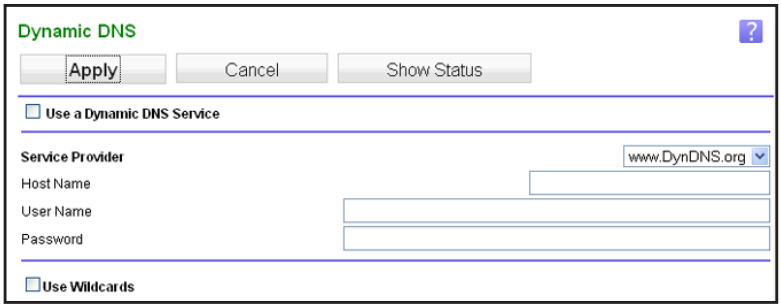
If your ISP assigns a private WAN IP address (such as 192.168.x.x or 10.x.x.x), the Dynamic DNS service does not work because private addresses are not routed on the Internet.

Your modem router contains a client that can connect to the Dynamic DNS service provided by DynDNS.org. If you register for an account and set up the modem router, whenever your ISP-assigned IP address changes, your modem router automatically contacts the Dynamic DNS service provider, logs in to your account, and registers your new IP address. If your host

name is hostname, for example, you can reach your modem router at http://hostname.dyndns.org.

➢ **To set up Dynamic DNS:**

1. Register for an account with one of the Dynamic DNS service providers whose URLs appear in the Service Provider list.
2. Select **Advanced > Dynamic DNS**.



3. Select the **Use a Dynamic DNS Service** check box.
4. Select the URL of your Dynamic DNS service provider. For example, for DynDNS.org, select **www.dyndns.org**.
5. Type the host name (or domain name) that your Dynamic DNS service provider gave you.
6. Type the user name for your Dynamic DNS account. This is the name that you use to log in to your account, not your host name.
7. Type the password (or key) for your Dynamic DNS account.
8. Click **Apply** to save your configuration.

Static Routes

Static routes provide additional routing information to your modem router. Typically, you do not need to add static routes. You have to configure static routes only for unusual cases such as multiple modem routers or multiple IP subnets on your network.

As an example of when a static route is needed, consider the following case:

- Your primary Internet access is through a cable modem to an ISP.
- You have an ISDN modem router on your home network for connecting to the company where you are employed. This modem router's address on your LAN is 192.168.0.100.
- Your company's network address is 134.177.0.0.

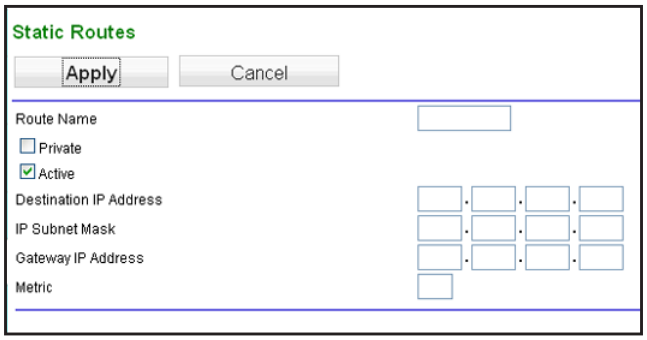
When you first configured your modem router, two implicit static routes were created. A default route was created with your ISP as the gateway, and a second static route was created to your local network for all 192.168.0.x addresses. With this configuration, if you attempt to access a device on the 134.177.0.0 network, your modem router forwards your request to the ISP. The ISP forwards your request to the company where you are employed, and the request is likely to be denied by the company's firewall.

In this case you have to define a static route, telling your modem router to access 134.177.0.0 through the ISDN modem router at 192.168.0.100. In this example:

- The Destination IP Address and IP Subnet Mask fields specify that this static route applies to all 134.177.x.x addresses.
- The Gateway IP Address field specifies that all traffic for these addresses should be forwarded to the ISDN modem router at 192.168.0.100.
- A metric value of 1 works since the ISDN modem router is on the LAN.
- Private is selected only as a precautionary security measure in case RIP is activated.

➢ **To set up a static route:**

1. Select **Advanced > Static Routes**, and click **Add** to display the following screen:



2. In the Route Name field, type a name for this static route (for identification purposes only.)
3. Select the **Private** check box if you want to limit access to the LAN only. If Private is selected, the static route is not reported in RIP.
4. Select the **Active** check box to make this route effective.
5. Type the destination IP address of the final destination.
6. Type the IP subnet mask for this destination. If the destination is a single host, type **255.255.255.255**.
7. Type the gateway IP address, which has to be a modem router on the same LAN segment as the modem router.
8. Type a number from 1 through 15 as the metric value.

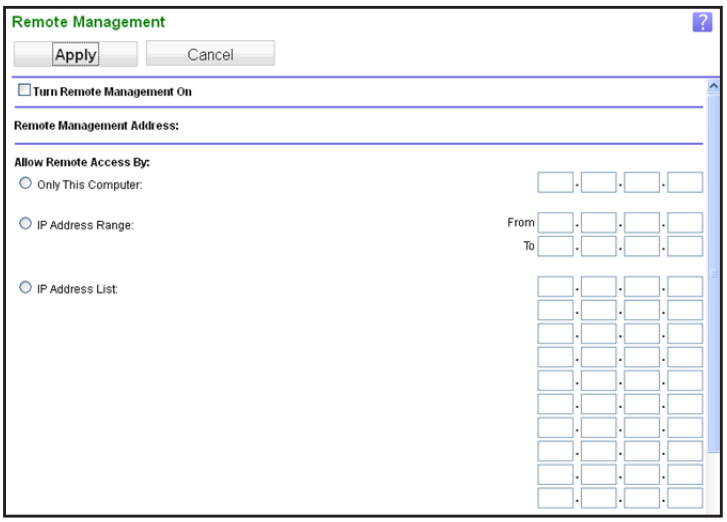
   This value represents the number of modem routers between your network and the destination. Usually, a setting of 2 or 3 works, but if this is a direct connection, set it to 1.
9. Click **Apply** to add the static route.

Remote Management

The remote management feature lets you upgrade or check the status of your N300RM Modem Router over the Internet.

➢ **To set up remote management:**

1. Select **Advanced > Remote Management**.



Note: *Be sure to change the modem router's default login password to a secure password. The ideal password contains no dictionary words from any language and contains upper-case and lower-case letters, numbers, and symbols. It can be up to 30 characters.*

2. Select the **Turn Remote Management On** check box.
3. Under Allow Remote Access By, specify the external IP addresses to be allowed to access the modem router's remote management.

Note: For enhanced security, restrict access to as few external IP addresses as practical.

- To allow access from a single IP address on the Internet, select **Only This Computer**. Enter the IP address that will be allowed access.
- To allow access from a range of IP addresses on the Internet, select **IP Address Range**. Enter a beginning and ending IP address to define the allowed range.
- To specify IP addresses, select **IP Address List** and type in the allowed IP addresses.
- To allow access from any IP address on the Internet, select **Everyone**.

4. Specify the port number for accessing the web management interface.

   Normal web browser access uses the standard HTTP service port 80. For greater security, enter a custom port number for the remote web management interface. Choose a number from 1024 to 65535, but do not use the number of any common service port. The default is 8080, which is a common alternate for HTTP.

5. Click **Apply** to have your changes take effect.
6. When accessing your modem router from the Internet, type your modem router's WAN IP address into your browser's address or location field followed by a colon (:) and the custom port number. For example, if your external address is 134.177.0.123 and you use port number 8080, enter **http://134.177.0.123:8080** in your browser.

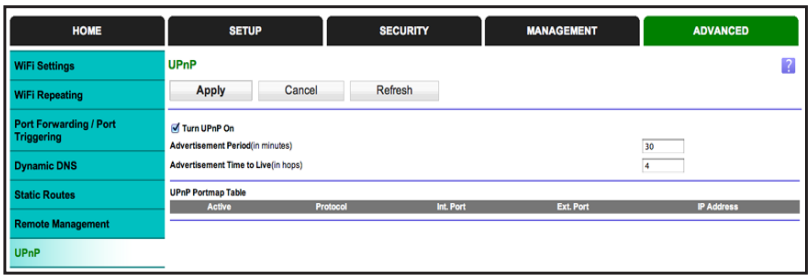
Universal Plug and Play

Universal Plug and Play (UPnP) helps devices, such as Internet appliances and computers, to access the network and connect to other devices as needed. UPnP devices can automatically discover the services from other registered UPnP devices on the network.

If you use applications such as multiplayer gaming, peer-to-peer connections, or real-time communications such as instant messaging or remote assistance (a feature in Windows XP), you should enable UPnP.

➢ **To turn on Universal Plug and Play:**

1. Select **Advanced > UPnP**. The UPnP screen displays.



2. Specify the settings.

   The available settings and information in this screen are:

   Turn UPnP On. UPnP can be enabled or disabled for automatic device configuration. The default setting for UPnP is disabled. If this check box is not selected, the modem router does not allow any device to automatically control the resources, such as port forwarding (mapping) of the modem router.

   Advertisement Period. The advertisement period is how often the modem router broadcasts its UPnP information. This value can range from 1 to 1440 minutes. The default period is 30 minutes. Shorter durations ensure that control points have current device status at the expense of additional network traffic. Longer durations can compromise the freshness of the device status, but can significantly reduce network traffic.

Advertisement Time to Live. The time to live for the advertisement is measured in hops (steps) for each UPnP packet sent. The time to live hop count is the number of steps a broadcast packet is allowed to propagate for each UPnP advertisement before it disappears. The number of hops can range from 1 to 255. The default value for the advertisement time to live is 4 hops, which is fine for most home networks. If you notice that some devices are not being updated or reached correctly, then it might be necessary to increase this value.

UPnP Portmap Table. The UPnP Portmap Table displays the IP address of each UPnP device that is currently accessing the modem router and which ports (internal and external) that device has opened. The UPnP Portmap Table also displays what type of port is open and whether that port is still active for each IP address.

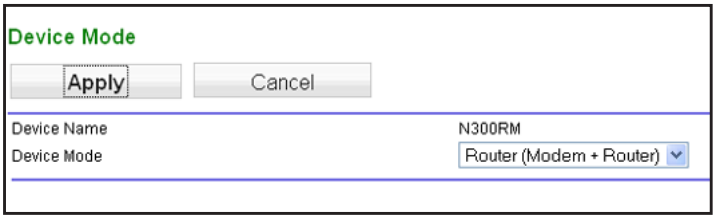
3. Click **Apply** to save your settings.

Change the Device Mode

The modem includes a built-in router. If you want to configure the modem as a “pure bridge” in Modem mode, first set up the Internet connection and then change the Device Mode setting to Modem mode. In Modem mode, the device acts as a “pure bridge” or DSL modem. When the device is in Modem mode, features that are not available are grayed out.

➢ **To change the device mode:**

1. Select **Advanced > Device Mode**. The following screen displays:



By default, the modem is in Router mode.

2. Select the device mode that you want from the drop-down list.
3. Click **Apply** so that your changes take effect.

Virtual Private Networking

7

VPN setup

This chapter contains the following sections:

- *Set Up a Gateway-to-Gateway VPN Configuration*
- *VPN Wizard*
- *Activate the VPN Tunnel*
- *Verify the Status of a VPN Tunnel*
- *Use Auto Policy to Configure VPN Tunnels*
- *Use Manual Policy to Configure VPN Tunnels*

Set Up a Gateway-to-Gateway VPN Configuration

Two common scenarios for VPN tunnels are between a remote computer and a network gateway, and between two or more network gateways. Gateway-to-gateway VPN tunnels provide secure access between networks, such as a branch or home office and a main office.

A VPN between two or more VPN-enabled routers is a good way to connect branch or home offices and business partners over the Internet. VPN tunnels also enable access to network resources across the Internet. In this case, use gateways on each end of the tunnel to form the VPN tunnel end points.

Set the LAN IPs on each modem router to a different subnet and configure each correctly for the Internet. The following table shows an example.

Table 3. Gateway-to-gateway VPN tunnel configuration

Parameter		**Value to Be Entered**	**Field Selection**	
Connection Name		GtoGr	N/A	
Pre-Shared Key		12345678	N/A	
Secure Association		N/A	Main Mode	Manual Keys
Perfect Forward Secrecy		N/A	Enabled	Disabled
Encryption Protocol		N/A	DES	3DES
Authentication Protocol		N/A	MD5	SHA-1
Diffie-Hellman (DH) Group		N/A	Group 1	Group 2
Key Life in seconds		28800 (8 hours)	N/A	
IKE Life Time in seconds		3600 (1 hour)	N/A	
VPN Endpoint	**Local IPSecID**	**LAN IP Address**	**Subnet Mask**	**FQDN or Gateway IP (WAN IP Address)**
Gateway_A	GW_A	192.168.0.1	255.255.255.0	14.15.16.17
Gateway_B	GW_B	192.168.3.1	255.255.255.0	22.23.24.25

The LAN IP address ranges of the VPN endpoints have to be different. The connection will fail if both are using the default address range of 192.168.0.x.

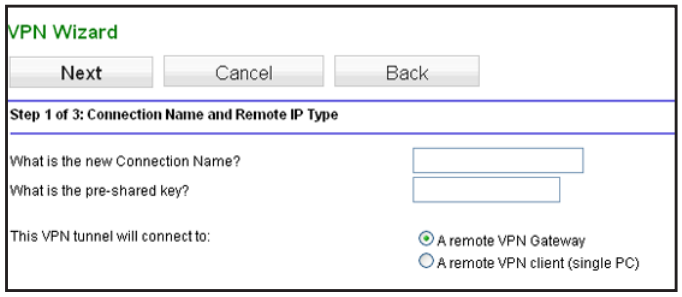
VPN Wizard

The VPN Wizard automates many of the steps in setting up a VPN tunnel. If you do not want to use the VPN Wizard or its default settings are not appropriate for your circumstances, use one of these alternatives:

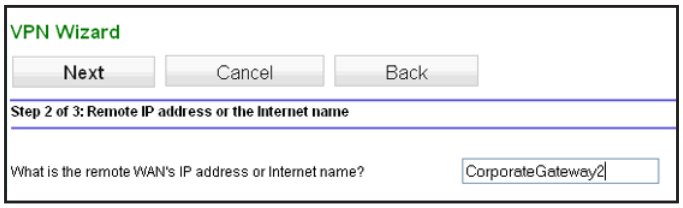
- **Auto Policy**. Auto Policy uses the IKE protocol to define the authentication scheme and automatically generate the encryption keys. See *Use Auto Policy to Configure VPN Tunnels* on page 88.
- **Manual Policy**. Manually enter the authentication and key parameters. See *Use Manual Policy to Configure VPN Tunnels* on page 91.

➢ **To configure a gateway-to-gateway VPN tunnel using the VPN Wizard:**

1. Select **Advanced > VPN Wizard** and click **Next**.
2. Fill in the Connection Name field and pre-shared key field.

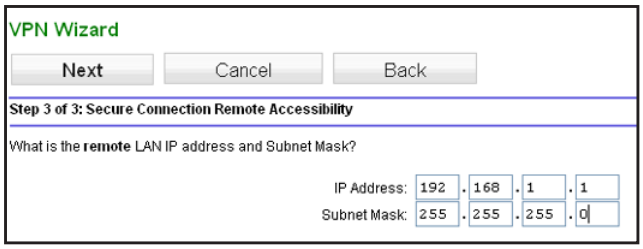


3. Select the **A remote VPN Gateway** radio button and click **Next**.
4. Fill in the IP address or FQDN for the target VPN endpoint WAN connection, and click **Next**.

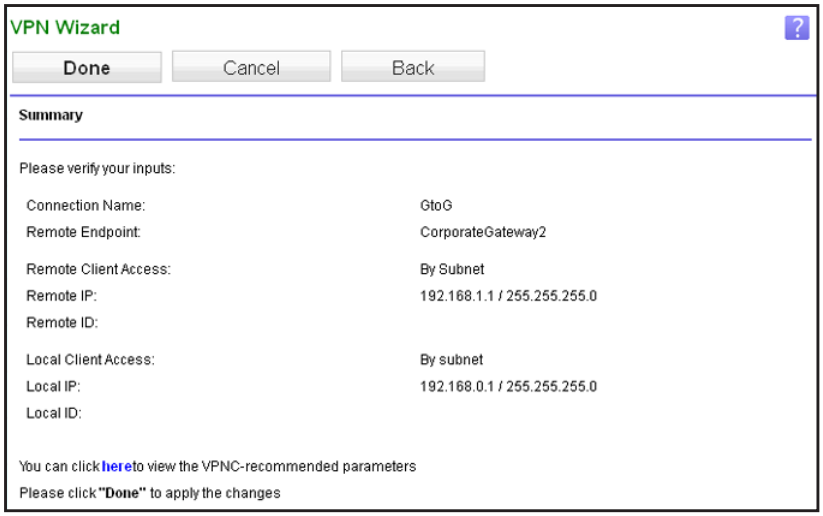


5. Fill in the IP Address and Subnet Mask fields for the target endpoint that can use this tunnel, and click **Next**.

6. Specify the local LAN address and subnet mask, and click **Next**.

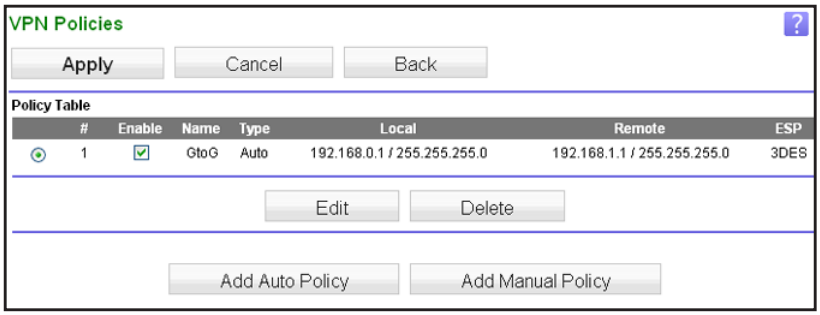


The VPN Wizard Summary screen displays:



7. Click **Done**.

The VPN Policies screen displays, showing that the new tunnel is enabled.



8. Repeat these steps for the second gateway, and pay special attention to the following network settings:
   - WAN IP address of the remote VPN gateway (for example, **14.15.16.17**)
   - LAN IP settings of the remote VPN gateway:
     - IP address (for example, **192.168.0.1**)
     - Subnet mask (for example, **255.255.255.0**)
     - Pre-shared key (for example, **12345678**)

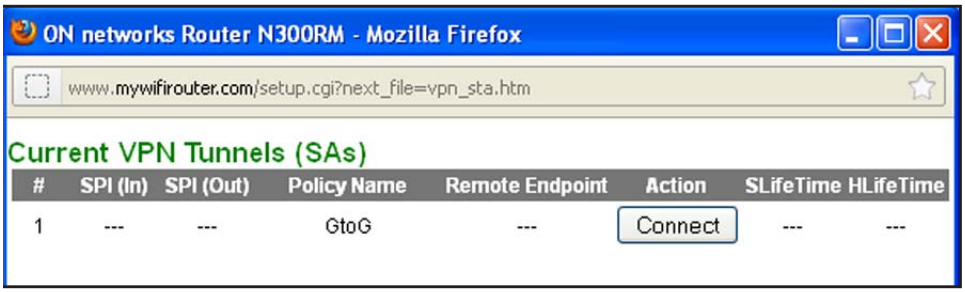
Activate the VPN Tunnel

There are three ways to activate theVPN tunnel:

- Use the VPN Status screen.
- Ping the remote endpoint.
- Start using the VPN tunnel.

➢ **To activate the VPN tunnel from the VPN Status screen:**

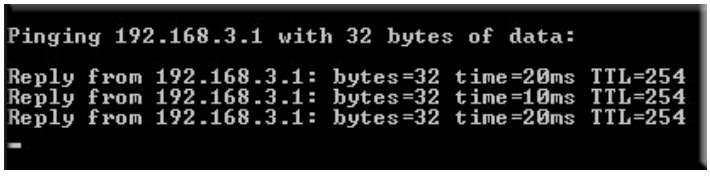
1. Select **Advanced > VPN Status**.
2. Click the **VPN Status** button to display the Current VPN Tunnels (SAs) screen:



3. Click **Connect** for the VPN tunnel that you want to activate. View the VPN Status/Log screen to verify that the tunnel is connected.

➢ **To activate the VPN tunnel by pinging the remote endpoint:**

1. Test the VPN tunnel by pinging the remote network from a computer attached to Gateway A (the modem router).
2. Open a command prompt (for example, **Start > Run > cmd**).
3. Type **ping 192.168.3.1** (substituting the endpoint of your remote gateway).



The pings might fail the first time. If they do, then try the pings a second time.

➢ **To use a VPN tunnel to activate the VPN tunnel:**

Use a web browser to go to a URL whose IP address or range is covered by the policy for that VPN tunnel.

Verify the Status of a VPN Tunnel

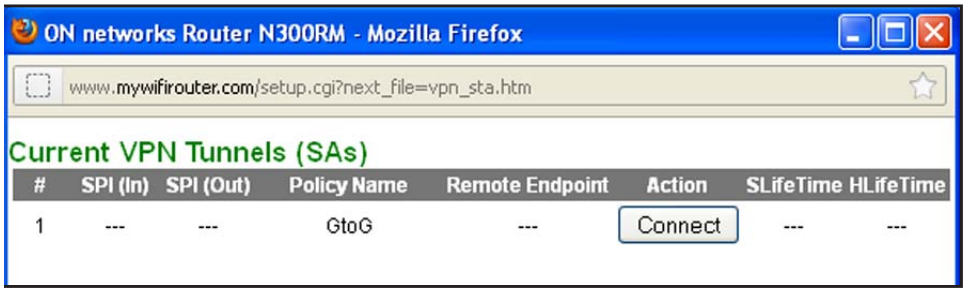
The VPN Status screen includes a log that shows the details of recent VPN activity, including the building of the VPN tunnel. If there is a problem with the VPN tunnel, refer to the log for information about what might be the cause of the problem.

➢ **To check the VPN tunnel status:**

1. Select **Advanced > VPN Status**.

   You can click **Refresh** to see the most recent entries, and you can click **Clear Log** to delete all log entries.

2. Click the **VPN Status** button to display the Current VPN Tunnels (SAs) screen.



This table lists the following data for each active VPN tunnel.

- **SPI**. Each SA has a unique SPI (security parameter index) for traffic in each direction. For manual key exchange, the SPI is specified in the policy definition. For automatic key exchange, the SPI is generated by the IKE protocol.
- **Policy Name**. The VPN policy associated with this SA.
- **Remote Endpoint**. The IP address on the remote VPN endpoint.
- **Action**. Either a Drop or a Connect button.
- **SLifeTime (Secs)**. The remaining soft lifetime for this SA in seconds. When the soft lifetime becomes 0 (zero), the SA (security association) is re-negotiated.
- **HLifeTime (Secs)**. The remaining hard lifetime for this SA in seconds. When the hard lifetime becomes 0 (zero), the SA (security association) is terminated. (It is re-established if required.)

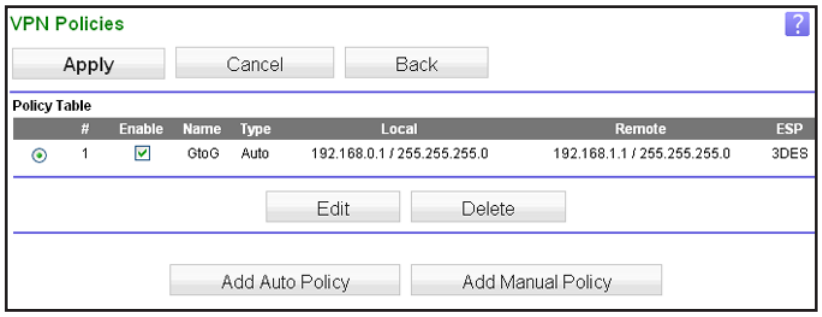
Deactivate a VPN Tunnel

Sometimes a VPN tunnel has to be deactivated for testing purposes. You can deactivate a VPN tunnel from two places:

- Policy Table on the VPN Policies screen
- VPN Status screen

- **To use the Policy Table to deactivate a VPN tunnel:**

1. Select **Advanced > VPN Policies**.

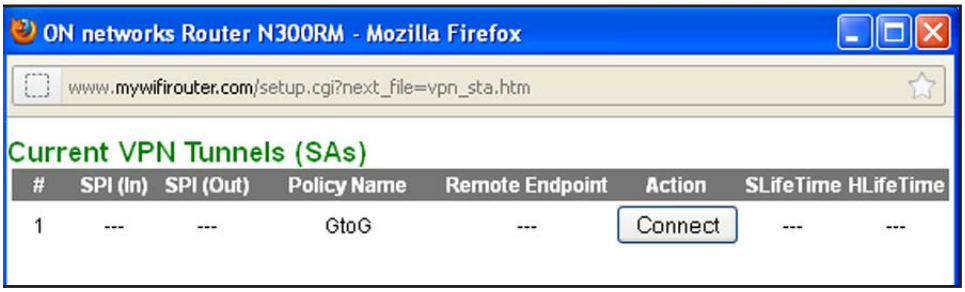


2. In the Policy Table, clear the **Enable** check box for the VPN tunnel that you want to deactivate.
3. Click **Apply**.

To reactivate the tunnel, select the **Enable** check box, and then click **Apply**.

- **To use the VPN Status screen to deactivate a VPN tunnel:**

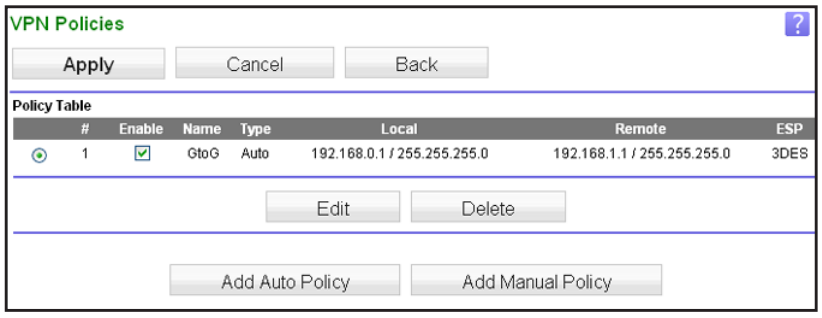
1. **Advanced > VPN Status**.
2. Click the **VPN Status** button.



3. Click **Drop** for the VPN tunnel that you want to deactivate.

- **To deactivate a VPN tunnel:**

1. Select **Advanced > VPN Policies**.



2. In the Policy Table, select the radio button for the VPN tunnel to be deleted
3. Click **Delete**.

Use Auto Policy to Configure VPN Tunnels

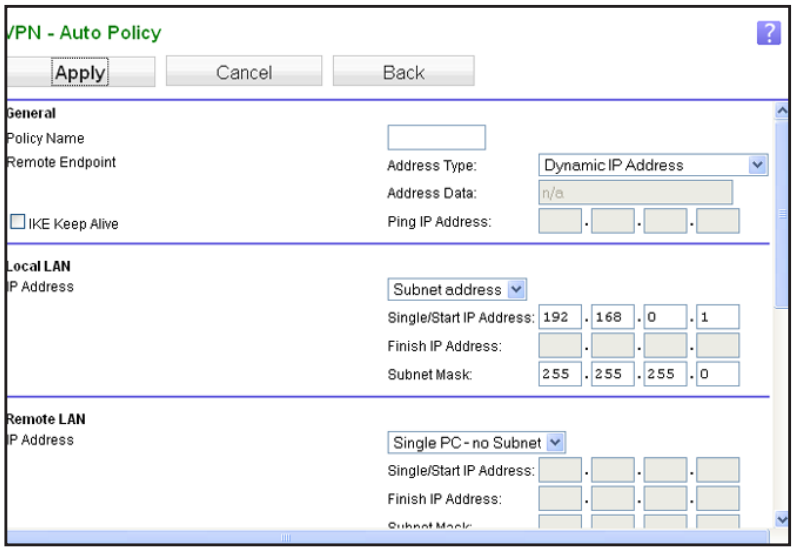
You need to configure matching VPN settings on both VPN endpoints. The outbound VPN settings on one end have to match to the inbound VPN settings on other end, and vice versa.

All VPN tunnels on the modem router require that you configure several network parameters. This section describes those parameters and how to access them.

The most common configuration scenarios use IKE to manage the authentication and encryption keys. The IKE protocol performs negotiations between the two VPN endpoints to generate and update the required encryption parameters.

➢ **To configure VPN network parameters:**

1. Select **Advanced > VPN Policies**.
2. Click the **Add Auto Policy**.



The VPN tunnel network connection fields are defined in the following sections.

VPN Auto Policy General Settings

- **Policy Name**. Enter a unique name. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
- **Remote VPN Endpoint**. The remote VPN endpoint has to have this VPN gateway's address entered as its remote VPN endpoint.

  If the remote endpoint has a dynamic IP address, select **Dynamic IP Address**. No address data input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select an option (**IP address** or **domain name**) and enter the address of the remote VPN endpoint to which you want to connect.

- **IKE Keep Alive**. If you want to ensure that a connection is kept open, or, if that is not possible, that it is quickly re-established when a connection is lost select this check box.

  The ping IP address has to be associated with the remote endpoint. You have to use the remote LAN address. This IP address will be pinged periodically to generate traffic for the VPN tunnel. The remote keep-alive IP address needs to be covered by the remote LAN IP range and to correspond to a device that can respond to a ping. The range should be made as narrow as possible to meet this objective.

VPN Auto Policy Local LAN Settings

The remote VPN endpoint needs to have these IP addresses entered as its remote addresses.

- **Subnet Mask**. The network mask.
- **Single/Start IP Address**. Enter the IP address for a single address, or the starting address for an address range. A single address setting is used when you want to make a single server on your LAN available to remote users. A range has to be an address range used on your LAN.
- **Any**. The remote VPN endpoint might be at any IP address.
- **Finish IP Address**. For an address range, enter the finish IP address. This needs to be an address range used on your LAN.

VPN Auto Policy Remote LAN Settings

The remote VPN endpoint has to have these IP addresses entered as its local addresses.

- **IP Address**. If there is no LAN (only a single computer) at the remote endpoint, select **Single PC - no Subnet** option. If this option is selected, no additional data is required. The typical application is a computer running the VPN client at the remote end.
- **Single/Start IP Address**. Enter an IP address that is on the remote LAN. You can use this setting when you want to access a server on the remote LAN.
  - For a range of addresses, enter the starting IP address. This needs to be an address range used on the remote LAN.
  - **Any**. Any outgoing traffic from the computers in the Local IP fields triggers an attempted VPN connection to the remote VPN endpoint. Be sure you want this option before selecting it.
- **Finish IP Address**. Enter the finish IP address for a range of addresses. This has to be an address range used on the remote LAN.
- **Subnet Mask**. Enter the network mask.

VPN Auto Policy IKE Settings

- **Direction**. This setting is used when the modem router determines if the IKE policy matches the current traffic. Select an option.
  - **Responder only**. Incoming connections are allowed, but outgoing connections are blocked.

  - **Initiator and Responder**. Both incoming and outgoing connections are allowed.
- **Exchange Mode**. Ensure that the remote VPN endpoint is set to use Main mode.
- **Diffie-Hellman (DH) Group**. The Diffie-Hellman algorithm is used when keys are exchanged. The DH Group setting determines the bit size used in the exchange. This value needs to match the value used on the remote VPN gateway.
- **Local Identity Type**. Select an option to match the Remote Identity Type setting on the remote VPN endpoint.
  - **WAN IP Address**. Your Internet IP address.
  - **Fully Qualified Domain Name**. Your domain name.
  - **Fully Qualified User Name**. Your name, email address, or other ID.
  - **Local Identity Data**. Enter the data for the local identity type that you selected. (If WAN IP Address is selected, no input is required.)
- **Remote Identity Type**. Select the option that matches the Local Identity Type setting on the remote VPN endpoint.
  - **IP Address**. The Internet IP address of the remote VPN endpoint.
  - **Fully Qualified Domain Nam**e. The domain name of the remote VPN endpoint.
  - **Fully Qualified User Name**. The name, email address, or other ID of the remote VPN endpoint.
  - **Remote Identity Data**. Enter the data for the remote identity type that you selected. If IP Address is selected, no input is required.

VPN Auto Policy Parameters

- **Encryption Algorithm**. The encryption algorithm used for both IKE and IPSec. This setting has to match the setting used on the remote VPN gateway. DES and 3DES are supported.
  - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.
  - **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- **Authentication Algorithm**. The authentication algorithm used for both IKE and IPSec. This setting has to match the setting used on the remote VPN gateway. Auto, MD5, and SHA-1 are supported. Auto negotiates with the remote VPN endpoint and is not available in responder-only mode.
  - **MD5**. 128 bits, faster but less secure.
  - **SHA-1**. 160 bits, slower but more secure. This is the default.
- **Pre-shared Key**. The key has to be entered both here and on the remote VPN gateway.
- **SA Life Time**. The time interval before the SA (security association) expires. (It is automatically reestablished as required.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA life time. This setting applies to both IKE and IPSec SAs.

- **Enable IPSec PFS (Perfect Forward Secrecy)**. If this check box is selected, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)

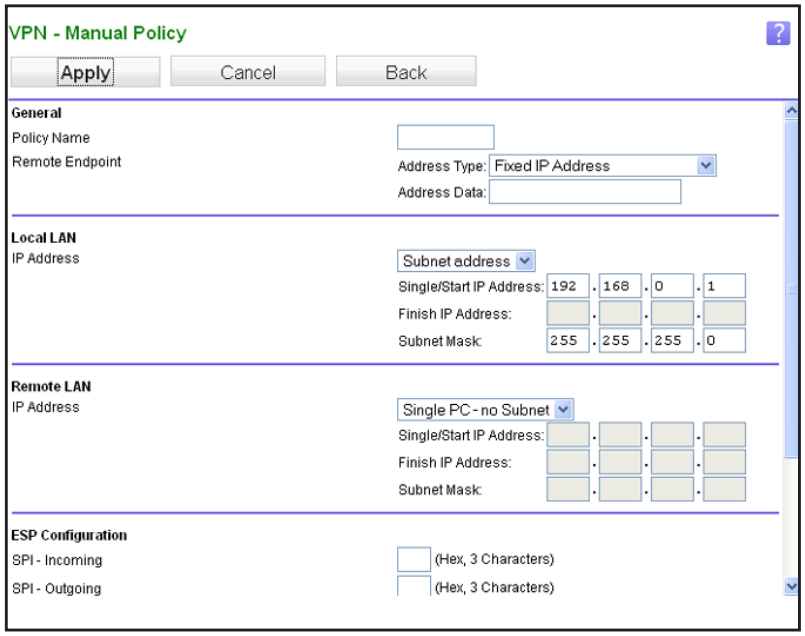
  This setting applies to both IKE and IPSec SAs. When configuring the remote endpoint to match this setting, you might have to specify the key group used. For this device, the key group is the same as the DH Group setting in the IKE section.

Use Manual Policy to Configure VPN Tunnels

As an alternative to IKE, you can use manual keying, in which you need to specify each phase of the connection. A manual VPN policy requires all settings for the VPN tunnel to be manually input at each end (both VPN endpoints).

➢ **To create a policy manually:**

1. Select **Advanced VPN Policies**.
2. On the VPN Policy screen, click the **Add Manual Policy** radio button.



The following sections explain the fields in the VPN Manual Policy screen.

VPN Manual Policy General Settings

The VPN tunnel network connection fields are as follows.

- **Policy Name**. Enter a unique name to identify this policy. This name is not supplied to the remote VPN endpoint. It is used only to help you manage the policies.
- **Remote VPN Endpoint**. The remote VPN endpoint has to have this VPN gateway's address entered as its remote VPN endpoint.

If the remote endpoint has a dynamic IP address, select **Dynamic IP Address**. No address data input is required. You can set up multiple remote dynamic IP policies, but only one such policy can be enabled at a time. Otherwise, select an option (**IP address** or **domain name**) and enter the address of the remote VPN endpoint to which you want to connect.

VPN Manual Policy Local LAN Settings

The remote VPN endpoint has to have these IP addresses entered as its remote addresses.

- **Subnet Address**. Enter the network mask.
- **Single PC - no Subnet**. Select this option if there is no LAN (only a single computer) at the remote endpoint. If this option is selected, no additional data is required.
- **Single/Start IP Address**. The IP address for a single address, or the starting address for an address range used on the LAN. If you want to make a single server on your LAN available to remote users, use a single address.
- **Any**. The remote VPN endpoint can be at any IP address.
- **Finish IP Address**. For an address range, enter the finish IP address. This has to be an address range used on your LAN.
- **Subnet Mask**. Enter the network mask.

VPN Manual Policy Remote LAN Settings

The remote VPN endpoint has to have these IP addresses entered as its local addresses.

- **IP Address**. Select **Single PC - no Subnet** if there is no LAN (only a single computer) at the remote endpoint. If this option is selected, no additional data is required. The typical application is a computer running the VPN client at the remote end.
- **Single/Start IP Address**. Enter an IP address on the remote LAN. You can use this setting to access a server.
  - For a range of addresses, enter the starting IP address. This has to be an address range used on the remote LAN.
  - **Any**. Any outgoing traffic from specified Local IP computers triggers an attempted VPN connection to the remote VPN endpoint. Be sure you want this option before selecting it.
- **Finish IP Address**. Enter the finish IP address for a range of addresses. This has to be an address range used on the remote LAN.
- **Subnet Mask**. Enter the network mask.

VPN Manual Policy ESP Settings

ESP (Encapsulating Security Payload) provides security for the payload (data) sent through the VPN tunnel.

- **SPI**. Enter the required security policy indexes (SPIs). Each policy has to have unique SPIs. These settings need to match the remote VPN endpoint. The **in** setting here has to

match the **out** setting on the remote VPN endpoint, and the **out** setting here has to match the **in** setting on the remote VPN endpoint.

- **Encryption**. Select an encryption algorithm, and enter the key in the field provided. For 3DES, the keys should be 24 ASCII characters, and for DES, the keys should be 8 ASCII characters.
  - **DES**. The Data Encryption Standard (DES) processes input data that is 64 bits wide, encrypting these values using a 56-bit key. Faster but less secure than 3DES.
  - **3DES**. (Triple DES) achieves a higher level of security by encrypting the data three times using DES with three different, unrelated keys.
- **Authentication**. Specify the authentication and the key.

Troubleshooting

8

Diagnose and solve problems

This chapter provides information about troubleshooting your N300 WiFi ADSL2+ Modem Router (N300RM). After each problem description, instructions are provided to help you diagnose and solve the problem.

> **Tip:** On Networks provides helpful articles, documentation, and the latest software updates at *http://www.on-networks.com/support*.

This chapter contains the following sections:

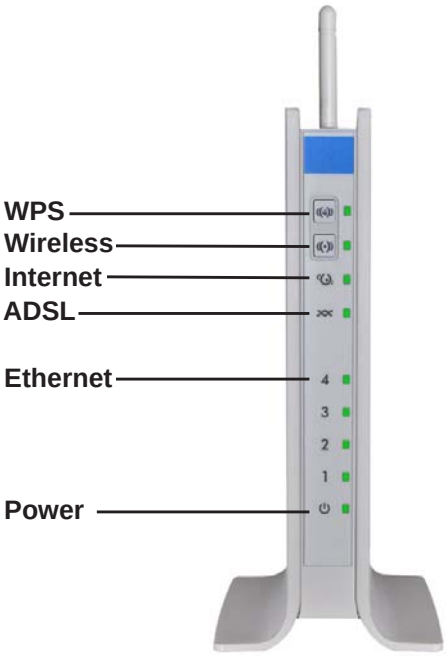
- *Troubleshoot with the LEDs*
- *Cannot Log In to the Modem Router*
- *Troubleshoot the Internet Connection*
- *TCP/IP Network Not Responding*
- *Changes Not Saved*
- *Incorrect Date or Time*

Troubleshoot with the LEDs

When you turn on the power, the Power, Ethernet, and ADSL LEDs light as described here. If they do not, refer to the sections that follow for help.

➢ **To check the LEDs:**

1. When power is first applied, the Power LED lights.
2. After approximately 10 seconds, the LAN and DSL LEDs light as follows:
   a. The Ethernet port LEDs light for any local ports that are connected.
   b. The ADSL link LED lights to indicate that there is a link to the connected device.



Power LED Is Off

If the Power and other LEDs are off when your modem router is turned on:

- Check that the power cord is correctly connected to your modem router and the power supply adapter is correctly connected to a functioning power outlet.
- Check that you are using the power adapter supplied in the package with this product.

If the error persists, you could have a hardware problem. Contact technical support.

Power LED Is Red

When the modem router is turned on, it performs a power-on self-test, during which time the Power LED turns red. If the Power LED does not turn green within a minute or so or if it turns red at any other time during normal operation, there is a fault within the modem router.

If the Power LED turns red to indicate a modem router fault, turn the power off and on to see if the modem router recovers. If the Power LED is still red 1 minute after power-up:

- Turn the power off and on one more time to see if the modem router recovers.
- Clear the modem router's configuration to factory defaults as explained in *Factory Settings* on page 103. Clearing the configuration sets the modem router IP address to 192.168.0.1.

If the error persists, you could have a hardware problem. Contact technical support.

Ethernet LED Is Off

If the appropriate LAN LED does not light when the Ethernet connection is made, check the following:

- The Ethernet cable connections are secure at the modem router and at the hub or workstation.
- The power is turned on to the connected hub or workstation.
- You are using the correct cable.

Cannot Log In to the Modem Router

If you are unable to log in to the modem router from a computer on your local network, check the following:

- If you are using an Ethernet-connected computer, check the Ethernet connection between the computer and the modem router as described in the previous section.
- Make sure that your computer IP address is on the same subnet as the modem router. If you are using the recommended addressing scheme, your computer address is in the range of 192.168.0.2 to 192.168.0.254.
- If your computer IP address is shown as 169.254.x.x, recent versions of Windows and Mac OS generate and assign an IP address if the computer cannot reach a DHCP server. These auto-generated addresses are in the range of 169.254.x.x. If your IP address is in this range, check the connection from the computer to the modem router, and reboot your computer.
- If your modem router's IP address was changed and you do not know the current IP address, clear the modem router's configuration to factory defaults. Resetting to factory defaults sets the modem router's IP address to 192.168.0.1. This procedure is explained in *Factory Settings* on page 103.
- Make sure that your browser has Java, JavaScript, or ActiveX enabled. If you are using Internet Explorer, click **Refresh** to be sure that the Java applet is loaded.
- Try quitting the browser and launching it again.
- Make sure that you are using the correct login information. The factory default login name is **admin**, and the password is **password**. Make sure that Caps Lock is off when you enter this information.

Troubleshoot the Internet Connection

If your modem router is unable to access the Internet, check the ADSL connection, then the WAN TCP/IP connection.

ADSL Link

If your modem router is unable to access the Internet, first determine whether you have an ADSL link with the service provider. The state of this connection is indicated with the ADSL LED.

ADSL Link LED Is Green

If your ADSL link LED is green, then you have a good ADSL connection. You can be confident that the service provider has connected your line correctly and that your wiring is correct.

ADSL Link LED Is Blinking Green

If your ADSL link LED is blinking green, then your modem router is attempting to make an ADSL connection with the service provider. The LED turns green within several minutes.

If the ADSL link LED does not turn green, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you are able to connect all your telephones.

If disconnecting telephones does not result in a green ADSL link LED, there might be a problem with your wiring. If the telephone company has tested the DSL signal at your network interface device (NID), then you might have poor-quality wiring in your house.

ADSL Link LED Is Off

If the ADSL link LED is off, disconnect all telephones on the line. If this solves the problem, reconnect the telephones one at a time, being sure to use a microfilter on each telephone. If the microfilters are connected correctly, you are able to connect all your telephones.

If disconnecting telephones does not result in a green ADSL link LED, check for the following:

- Check that the telephone company has made the connection to your line and tested it.
- Verify that you are connected to the correct telephone line. If you have more than one phone line, be sure that you are connected to the line with the ADSL service. It might be necessary to use a swapper if your ADSL signal is on pins 1 and 4 or the RJ-11 jack. The modem router uses pins 2 and 3.

Internet LED Is Red

If the Internet LED is red, the device was unable to connect to the Internet. Verify the following:

- Check that your login credentials are correct, or that the information you entered on the Basic Settings screen is correct.
- Check with your ISP to verify that the multiplexing method, VPI, and VCI settings on the ADSL Settings screen are correct.
- Check if your ISP has a problem—it might not be that the modem router cannot connect to the Internet, but rather that your ISP that cannot provide an Internet connection.

Obtain an Internet IP Address

If your modem router is unable to access the Internet, and your Internet LED is green, see if the modem router can obtain an Internet IP address from the ISP. Unless you have been assigned a static IP address, your modem router requests an IP address from the ISP. You can determine whether the request was successful using the browser interface.

➢ **To check the Internet IP address from the browser interface:**

1. Launch your browser, and select an external website.
2. Access the main menu of the modem router's configuration at http://192.168.0.1.
3. On the Home screen (Router Status) check that an IP address is shown for the WAN port. If 0.0.0.0 is shown, your modem router has not obtained an IP address from your ISP.

If your modem router is unable to obtain an IP address from the ISP, the problem might be one of the following:

- If you have selected a login program, the service name, user name, or password might be incorrectly set. See the following section, *Troubleshoot PPPoE or PPPoA*.
- Your ISP might check for your computer host name. Assign the computer host name of your ISP account to the modem router in the browser-based Setup Wizard.
- Your ISP allows only one Ethernet MAC address to connect to Internet, and might check for your computer MAC address. In this case, do one of the following:
  - Inform your ISP that you have bought a new network device, and ask them to use the modem router's MAC address.
  - Configure your modem router to spoof your computer MAC address. This configuration can be done in the Basic Settings screen.

Troubleshoot PPPoE or PPPoA

➢ **To debug the PPPoE or PPPoA connection:**

1. Log in to the modem router at http://192.168.0.1.
2. On the Home screen, click the **Connection Status** button.

3. If all of the steps indicate OK, then your PPPoE or PPPoA connection is up and working.
4. If any of the steps indicates Failed, you can attempt to reconnect by clicking **Connect**. The modem router continues to attempt to connect indefinitely.

If you cannot connect after several minutes, you might be using an incorrect service name, user name, or password. Also, there might be a provisioning problem with your ISP.

Note: Unless you connect manually, the modem router does not authenticate using PPPoE or PPPoA until data is transmitted to the network.

Troubleshoot Internet Browsing

If your modem router can obtain an IP address, but your computer is unable to load any web pages from the Internet:

- Your computer might not recognize any DNS server addresses.

  A DNS server is a host on the Internet that translates Internet names (such as www addresses) to numeric IP addresses. Typically your ISP provides the addresses of one or two DNS servers for your use. If you entered a DNS address when you set up the modem router, reboot your computer, and verify the DNS address. Alternatively, you can configure your computer manually with DNS addresses, as explained in your operating system documentation.

- Your computer might not have the modem router configured as its TCP/IP modem router.

  If your computer obtains its information from the modem router by DHCP, reboot the computer, and verify the modem router address.

TCP/IP Network Not Responding

Most TCP/IP terminal devices and routers have a ping utility for sending an echo request packet to the designated device. The device responds with an echo reply to tell whether a TCP/IP network is responding to requests.

Test the LAN Path to Your Modem Router

You can ping the modem router from your computer to verify that the LAN path to your modem router is set up correctly.

➢ **To ping the modem router from a computer running Windows 95 or later:**

1. From the Windows task bar, click the **Start** button, and select **Run**.
2. In the field provided, type **ping** followed by the IP address of the modem router, as in this example:

ping 192.168.0.1

3. Click **OK**.

   You see a message like this one:

   `Pinging <IP address> with 32 bytes of data`

   If the path is working, you see this message:

   `Reply from < IP address >: bytes=32 time=NN ms TTL=xxx`

   If the path is not working, you see this message:

   `Request timed out`

   If the path is not functioning correctly, you could have one of the following problems:

   - Wrong physical connections
     - Make sure that the Ethernet port LED is lit. If the LED is off, follow the instructions in *Ethernet LED Is Off* on page 96.
     - Check that the corresponding link LEDs are on for your network interface card and for the hub ports (if any) that are connected to your workstation and modem router.
   - Wrong network configuration
     - Verify that the Ethernet card driver software and TCP/IP software are both installed and configured on your computer or workstation.
     - Verify that the IP address for your modem router and your workstation are correct and that the addresses are on the same subnet.

Test the Path from Your Computer to a Remote Device

After you verify that the LAN path works correctly, test the path from your computer to a remote device. In the Windows Run screen, type:

`ping -n 10 IP address`

where *IP address* is the IP address of a remote device such as your ISP's DNS server.

If the path is functioning correctly, replies as described in *Test the LAN Path to Your Modem Router* on page 99 display. If you do not receive replies:

- Check that your computer has the IP address of your modem router listed as the default modem router. If the IP configuration of your computer is assigned by DHCP, this information is not visible in your computer Network Control Panel. Verify that the IP address of the modem router is listed as the default router.
- Check that the network address of your computer (the portion of the IP address specified by the netmask) is different from the network address of the remote device.
- Check that your cable or DSL modem is connected and functioning.
- If your ISP assigned a host name to your computer, enter that host name as the account name in the Basic Settings screen.

- Your ISP could be rejecting the Ethernet MAC addresses of all but one of your computers. Many broadband ISPs restrict access by allowing traffic only from the MAC address of your modem, but some additionally restrict access to the MAC address of a single computer connected to that modem. In this case, configure your modem router to clone or spoof the MAC address from the authorized computer.

Changes Not Saved

If the modem router does not save the changes you make in the modem router interface, check the following:

- When entering configuration settings, always click the **Apply** button before moving to another screen or tab, or your changes are lost.
- Click the **Refresh** or **Reload** button in the web browser. The changes might have occurred, but the old settings might be in the web browser cache.

Incorrect Date or Time

Select **Security > Schedule** to display the current date and time. The modem router uses the Network Time Protocol (NTP) to obtain the current time from one of several network time servers on the Internet. Each entry in the log is stamped with the date and time of day. Problems with the date and time function can include the following:

- Date shown is January 1, 2000. The modem router has not yet reached a network time server. Check that your Internet access is configured correctly. If you have finished setting up the modem router, wait at least 5 minutes, and check the date and time again.
- Time is off by one hour. This modem has automatic DST adjustment. To use this feature, in the Schedule screen, make sure the **Automatically adjust for daylight savings time** check box is selected.

Supplemental Information

A

This appendix covers the following topics:

- *Factory Settings*
- *Technical Specifications*

Factory Settings

You can return the modem router to its factory settings. Use the end of a paper clip or some other similar object to press and hold the **Reset** button for at least 7 seconds.

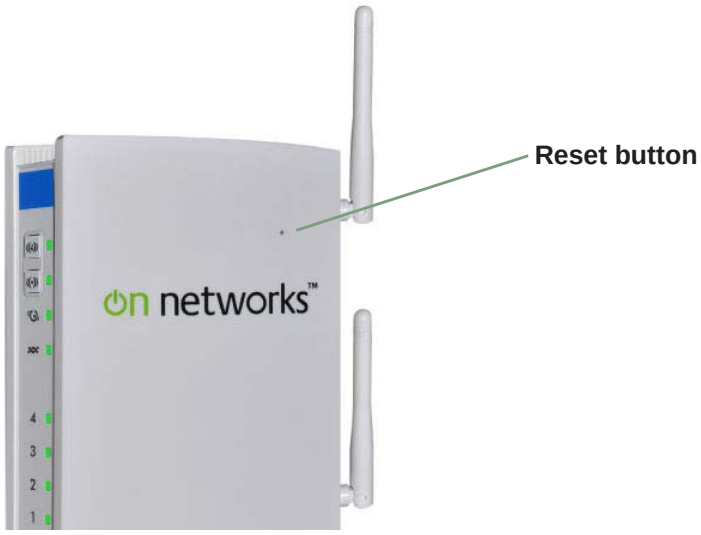


Figure 10. Reset button

The modem router resets, and returns to the factory settings, as shown in the following table.

Table 4. Factory default settings

Feature		Default Behavior
Router login	User login URL	http://www.mywifirouter.com
	User name (case-sensitive)	admin
	Login password (case-sensitive)	admin
Internet connection	WAN MAC address	Use default address
	WAN MTU size	1458
	Port speed	Autosensing
Local network (LAN)	LAN IP	192.168.0.1
	Subnet mask	255.255.255.0
	RIP direction	None
	RIP version	Disabled
	RIP authentication	None
	DHCP server	Enabled

Table 4. Factory default settings (continued)

Feature		Default Behavior
Local network (LAN) continued	DHCP starting IP address	192.168.0.2
	DHCP ending IP address	192.168.0.254
	DMZ	Enabled or disabled
	Time zone	GMT for WW except NA and GR, GMT+1 for GR, GMT-8 for NA
	Time zone adjusted for daylight savings time	Disabled
	SNMP	Disabled
Firewall	Inbound (communications coming in from the Internet)	Disabled (except traffic on port 80, the HTTP port)
	Outbound (communications going out to the Internet)	Enabled (all)
	Source MAC filtering	Disabled
Wireless	Wireless communication	Enabled
	SSID name	*OnNetworksXX* (where XX are two random digits) Can be found on the label on the bottom of the unit.
	WiFi password	*XXXXXXXX* (8 random digits)
	Security	Mixed WPA2-PSK
	Broadcast SSID	Enabled
	Country/region	Europe
	RF channel	Auto
	Operating mode	Up to 300 Mbps
	Data rate	Best
	Output power	Full
	Access point	Enabled
	Authentication type	Pre-Shared Key
	Wireless card access list	All wireless stations allowed

Technical Specifications

Table 5. Technical specifications

Feature	Description
Data and routing protocols	TCP/IP, RIP-1, RIP-2, DHCP, PPPoE or PPPoA, RFC 1483 Bridged or Routed Ethernet, and RFC 1577 Classical IP over ATM
AC plug is localized	110V-220V, 50/60 Hz, input
Dimensions	200 x 113.4 x 86.2 mm (7.9 x 4.5 x 3.4 in.)
Weight	0.2.85 kg (0.63 lb)
Operating temperature	0° to 40° C (32º to 104º F)
Operating humidity	90% maximum relative humidity, noncondensing
Regulatory compliance	EN 55022/24 (CISPR 22/24) Class B EN 60950 (CE LVD) Class B EN 301 489-17 V.2.1.1 (2009) EN 301 489-1 V1.9.2 (2011) EN 300 328 V1.7.1 (2006) K21:ITU-T K.21- 07/2003 TBR21: TBR21 January 1998
Interface specifications	LAN: 10BASE-T or 100BASE-Tx, RJ-45 WAN: ADSL, dual RJ-11, pins 2 and 3 T1.413, G.DMT, G.Lite ITU Annex A hardware or Annex B hardware ITU G.992.5 (ADSL2+)

Notification of Compliance

B

Wireless Routers, Gateways, APs

Regulatory Compliance Information

Note: This section includes user requirements for operating this product in accordance with National laws for usage of radio spectrum and operation of radio devices. Failure of the end-user to comply with the applicable requirements may result in unlawful operation and adverse action against the end-user by the applicable National regulatory authority.

Note: This product's firmware limits operation to only the channels allowed in a particular Region or Country. Therefore, all options described in this user's guide may not be available in your version of the product.

Europe – EU Declaration of Conformity

Marking by the above symbol indicates compliance with the Essential Requirements of the R&TTE Directive of the European Union (1999/5/EC). This equipment meets the following conformance standards:

EN300 328 (2.4Ghz), EN301 489-17 EN60950-1

For the EU Declarations of Conformity, visit *http://www.on-networks.com/doc.*

EDOC in Languages of the European Community

Language	Statement
Cesky [Czech]	*On Networks* tímto prohlašuje, že tento Radiolan je ve shode se základními požadavky a dalšími príslušnými ustanoveními smernice 1999/5/ES.
Dansk [Danish]	Undertegnede *On Networks* erklærer herved, at følgende udstyr Radiolan overholder de væsentlige krav og øvrige relevante krav i direktiv 1999/5/EF.
Deutsch [German]	Hiermit erklärt *On Networks* dass sich das Gerät Radiolan in Übereinstimmung mit den grundlegenden Anforderungen und den übrigen einschlägigen Bestimmungen der Richtlinie 1999/5/EG befindet.
Eesti [Estonian]	Käesolevaga kinnitab *On Networks* seadme Radiolan vastavust direktiivi 1999/5/EÜ põhinõuetele ja nimetatud direktiivist tulenevatele teistele asjakohastele sätetele.
English	Hereby, *On Networks* declares that this Radiolan is in compliance with the essential requirements and other relevant provisions of Directive 1999/5/EC.

Español [Spanish]	Por medio de la presente *On Networks* declara que el Radiolan cumple con los requisitos esenciales y cualesquiera otras disposiciones aplicables o exigibles de la Directiva 1999/5/CE.
Ελληνική [Greek]	ΜΕ ΤΗΝ ΠΑΡΟΥΣΑ *On Networks* ΔΗΛΩΝΕΙ ΟΤΙ Radiolan ΣΥΜΜΟΡΦΩΝΕΤΑΙ ΠΡΟΣ ΤΙΣ ΟΥΣΙΩΔΕΙΣ ΑΠΑΙΤΗΣΕΙΣ ΚΑΙ ΤΙΣ ΛΟΙΠΕΣ ΣΧΕΤΙΚΕΣ ΔΙΑΤΑΞΕΙΣ ΤΗΣ ΟΔΗΓΙΑΣ 1999/5/ΕΚ.
Français [French]	Par la présente *On Networks* déclare que l'appareil Radiolan est conforme aux exigences essentielles et aux autres dispositions pertinentes de la directive 1999/5/CE.
Italiano [Italian]	Con la presente *On Networks* dichiara che questo Radiolan è conforme ai requisiti essenziali ed alle altre disposizioni pertinenti stabilite dalla direttiva 1999/5/CE.
Latviski [Latvian]	Ar šo *On Networks* deklarē, ka Radiolan atbilst Direktīvas 1999/5/EK būtiskajām prasībām un citiem ar to saistītajiem noteikumiem.
Lietuvių [Lithuanian]	Šiuo *On Networks* deklaruoja, kad šis Radiolan atitinka esminius reikalavimus ir kitas 1999/5/EB Direktyvos nuostatas.
Nederlands [Dutch]	Hierbij verklaart *On Networks* dat het toestel Radiolan in overeenstemming is met de essentiële eisen en de andere relevante bepalingen van richtlijn 1999/5/EG.
Malti [Maltese]	Hawnhekk, *On Networks* jiddikjara li dan Radiolan jikkonforma mal-htigijiet essenzjali u ma provvedimenti ohrajn relevanti li hemm fid-Dirrettiva 1999/5/EC.
Magyar [Hungarian]	Alulírott, *On Networks* nyilatkozom, hogy a Radiolan megfelel a vonatkozó alapvetõ követelményeknek és az 1999/5/EC irányelv egyéb elõírásainak.
Polski [Polish]	Niniejszym On Networks oświadcza, że Radiolan jest zgodny z zasadniczymi wymogami oraz pozostałymi stosownymi postanowieniami Dyrektywy 1999/5/EC.
Português [Portuguese]	*On Networks* declara que este Radiolan está conforme com os requisitos essenciais e outras disposições da Directiva 1999/5/CE.
Slovensko [Slovenian]	On Networks izjavlja, da je ta Radiolan v skladu z bistvenimi zahtevami in ostalimi relevantnimi določili direktive 1999/5/ES.
Slovensky [Slovak]	*On Networks* týmto vyhlasuje, že Radiolan spĺňa základné požiadavky a všetky príslušné ustanovenia Smernice 1999/5/ES.
Suomi [Finnish]	*On Networks* vakuuttaa täten että Radiolan tyyppinen laite on direktiivin 1999/5/EY oleellisten vaatimusten ja sitä koskevien direktiivin muiden ehtojen mukainen.
Svenska [Swedish]	Härmed intygar *On Networks* att denna Radiolan står I överensstämmelse med de väsentliga egenskapskrav och övriga relevanta bestämmelser som framgår av direktiv 1999/5/EG.

Íslenska [Icelandic]	Hér með lýsir *On Networks* yfir því að Radiolan er í samræmi við grunnkröfur og aðrar kröfur, sem gerðar eru í tilskipun 1999/5/EC.
Norsk [Norwegian]	*On Networks* erklærer herved at utstyret *Radiolan* er i samsvar med de grunnleggende krav og øvrige relevante krav i direktiv 1999/5/EF.

This device is a 2.4 GHz wideband transmission system (transceiver), intended for use in all EU member states and EFTA countries, except in France and Italy where restrictive use applies.

In Italy the end-user should apply for a license at the national spectrum authorities in order to obtain authorization to use the device for setting up outdoor radio links and/or for supplying public access to telecommunications and/or network services.

This device may not be used for setting up outdoor radio links in France and in some areas the RF output power may be limited to 10 mW EIRP in the frequency range of 2454 - 2483.5 MHz. For detailed information the end-user should contact the national spectrum authority in France.

FCC Requirements for Operation in the United States

FCC Information to User

This product does not contain any user serviceable components and is to be used with approved antennas only. Any product changes or modifications will invalidate all applicable regulatory certifications and approvals.

FCC Guidelines for Human Exposure

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance of 20 cm between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

FCC Declaration of Conformity

We, On Networks 350 East Plumeria Drive, San Jose, CA 95134, declare under our sole responsibility that the N300 WiFi ADSL2+ Modem Router (N300RM) complies with Part 15 Subpart B of FCC CFR47 Rules. Operation is subject to the following two conditions:

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

FCC Radio Frequency Interference Warnings & Instructions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following methods:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an electrical outlet on a circuit different from that which the radio receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution

- Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate this equipment.
- This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

- For product available in the USA market, only channel 1~11 can be operated. Selection of other channels is not possible.
- This device and its antenna(s) must not be co-located or operation in conjunction with any other antenna or transmitter.

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (N300 WiFi ADSL2+ Modem Router (N300RM)) does not exceed the Class B limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

This Class [B] digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe [B] est conforme à la norme NMB-003 du Canada

Industry Canada

This device complies with RSS-210 of the Industry Canada Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

IMPORTANT NOTE: Radiation Exposure Statement:

This equipment complies with IC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

Caution:

Ce dispositif est conforme à la norme CNR-210 d'Industrie Canada applicable aux appareils radio exempts de licence. Son fonctionnement est sujet aux deux conditions suivantes: (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

NOTE IMPORTANTE: Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

Interference Reduction Table

The table below shows the Recommended Minimum Distance between On Networks equipment and household appliances to reduce interference (in feet and meters).

Household Appliance	Recommended Minimum Distance (in feet and meters)
Microwave ovens	30 feet / 9 meters
Baby Monitor - Analog	20 feet / 6 meters
Baby Monitor - Digital	40 feet / 12 meters
Cordless phone - Analog	20 feet / 6 meters
Cordless phone - Digital	30 feet / 9 meters
Bluetooth devices	20 feet / 6 meters
ZigBee	20 feet / 6 meters